Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-163734
Filing date: 01 June 2004 (01.06.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 Date of Application:	２００４年　６月　１日
出 願 番 号 Application Number:	特願２００４－１６３７３４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１６３７３４
出 願 人 Applicant(s):	松下電器産業株式会社

２００５年　４月１３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

【書類名】　特許願
【整理番号】　2048160209
【提出日】　平成16年 6月 1日
【あて先】　特許庁長官　殿
【国際特許分類】　G09L 1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　宮▲ざき▼　雅也
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　雅哉
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　村瀬　薫
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100090446
　【弁理士】
　【氏名又は名称】　中島　司朗
【先の出願に基づく優先権主張】
　【出願番号】　特願2004-110069
　【出願日】　平成16年 4月 2日
【先の出願に基づく優先権主張】
　【出願番号】　特願2004-146963
　【出願日】　平成16年 5月17日
【先の出願に基づく優先権主張】
　【出願番号】　特願2004-151621
　【出願日】　平成16年 5月21日
【手数料の表示】
　【予納台帳番号】　014823
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲 1

【物件名】　　明細書　1
【物件名】　　図面　1
【物件名】　　要約書　1
【包括委任状番号】　9003742

【書類名】特許請求の範囲
【請求項１】
　不正コンテンツを検知する不正コンテンツ検知システムであって、
　前記不正コンテンツ検知システムは、
前記コンテンツを、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、実行装置へ配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
　前記配布センタは、
　前記コンテンツを入力する入力部と、
　認証情報生成情報を保持する認証情報生成情報格納部と、
　前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
　前記コンテンツと、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
　前記実行装置は、
　前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を取得する取得部と、
　認証情報を検証するための検証情報を保持する検証情報格納部と、
　前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、
　前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
　を備えることを特徴とする不正コンテンツ検知システム。
【請求項２】
　前記コンテンツは、前記実行装置で実行可能なプログラムであり、
　前記実行部は、前記プログラムを実行すること、
　を特徴とする請求項１に記載の不正コンテンツ検知システム。
【請求項３】
　コンテンツを実行、もしくは再生する実行装置であって、
　前記実行装置は、
　前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、
　認証情報を検証するための検証情報を保持する検証情報格納部と、
　前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、
　前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
　を備えることを特徴とする実行装置。
【請求項４】
　前記取得部は、可搬媒体からデータを取得すること、
　を特徴とする、請求項３に記載の実行装置。
【請求項５】
　前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取

得すること、
を特徴とする、請求項３に記載の実行装置。
【請求項６】
前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、
を特徴とする、請求項３から請求項５のいずれか１項に記載の実行装置。
【請求項７】
前記実行装置は、さらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、
前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、
を特徴とする、請求項３から請求項６のいずれか１項に記載の実行装置。
【請求項８】
前記実行装置は、さらに、
前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、
前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、
を特徴とする、請求項７に記載の実行装置。
【請求項９】
前記実行装置は、さらに、
デバイス鍵を保持するデバイス鍵格納部と、
前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、
前記取得部はさらに、前記暗号化鍵束を受信すること、
を特徴とする、請求項７または請求項８に記載の実行装置。
【請求項１０】
前記取得部は、ｍ個（ｍは２以上の自然数）の前記コンテンツ位置情報と、前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応するｍ個の前記認証情報の中から、ｂ組（ｂは１以上ｍ－１以下の自然数）の前記コンテンツ位置情報及び前記認証情報を取得し、
前記検証部は、前記コンテンツ及びｍ個の前記コンテンツ位置情報を基に、ｍ個の前記代表部分コンテンツを取得し、ｍ個の前記代表部分コンテンツ及びｍ個の前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、
を特徴とする、請求項３から請求項９のいずれか１項に記載の実行装置。
【請求項１１】
前記取得部は、ｍ組の前記コンテンツ位置情報及び前記認証情報の中から、ｂ組の前記コンテンツ位置情報及び前記認証情報をランダムに選択すること、
を特徴とする、請求項１０に記載の実行装置。
【請求項１２】
前記取得部は、ｍ組の前記コンテンツ位置情報及び前記認証情報の中から、ｂ組の前記コンテンツ位置情報及び前記認証情報を順番に選択すること、
を特徴とする、請求項１０に記載の実行装置。
【請求項１３】
前記取得部において、ｂは１であること、
を特徴とする、請求項１０から請求項１２のいずれか１項に記載の実行装置。
【請求項１４】
前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、

を特徴とする、請求項３から請求項１３のいずれか１項に記載の実行装置。
【請求項１５】
前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、
を特徴とする、請求項３から請求項１３のいずれか１項に記載の実行装置。
【請求項１６】
前記検証情報は、デジタル署名方式の検証鍵であること、
を特徴とする、請求項３から請求項１３のいずれか１項に記載の実行装置。
【請求項１７】
前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、
前記取得部はさらに、前記検証情報識別子を受信し、
前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、
を特徴とする、請求項３から請求項１６のいずれか１項に記載の実行装置。
【請求項１８】
前記取得部はさらに、前記検証情報を受信すること、
を特徴とする、請求項３から請求項１７のいずれか１項に記載の実行装置。
【請求項１９】
前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、
前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、
を特徴とする、請求項１６から請求項１８のいずれか１項に記載の実行装置。
【請求項２０】
前記実行装置は、さらに、
前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、
を特徴とする、請求項１９に記載の実行装置。
【請求項２１】
前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、
を特徴とする、請求項２０に記載の実行装置。
【請求項２２】
前記第二取得部と前記取得部は等しいこと、
を特徴とする、請求項２０または請求項２１に記載の実行装置。
【請求項２３】
前記コンテンツは、前記実行装置で実行可能なプログラムであり、
前記実行部は、前記プログラムを実行すること、
を特徴とする請求項３から請求項２２のいずれか１項に記載の実行装置。
【請求項２４】
コンテンツを配布する配布センタであって、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、前記認証情報と、を配布する配布部と、
を備えることを特徴とする配布センタ。
【請求項２５】
前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、
を特徴とする、請求項２４に記載の配布センタ。
【請求項２６】
前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、
を特徴とする、請求項２４または請求項２５に記載の配布センタ。
【請求項２７】
前記配布センタはさらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、
前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、
を特徴とする、請求項２４から請求項２６のいずれか１項に記載の配布センタ。
【請求項２８】
前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする、請求項２７に記載の配布センタ。
【請求項２９】
前記配布センタはさらに
前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、
前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、
を特徴とする、請求項２７または請求項２８に記載の配布センタ。
【請求項３０】
前記コンテンツ位置情報格納部は、ｍ個（ｍは２以上の自然数）の前記コンテンツ位置情報及び前記コンテンツを保持し、
前記認証情報生成部は、ｍ個の前記コンテンツ位置情報及び前記コンテンツを基に、ｍ個の前記代表部分コンテンツを取得し、ｍ個の前記代表部分コンテンツ及び前記認証情報生成情報を基に、ｍ個の認証情報を生成し、
前記取得部は、前記コンテンツ位置情報と前記認証情報のｍ組を配布すること、
を特徴とする、請求項２４から請求項２９のいずれか１項に記載の配布センタ。
【請求項３１】
前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、
を特徴とする、請求項２４から請求項３０のいずれか１項に記載の配布センタ。
【請求項３２】
前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、
を特徴とする、請求項２４から請求項３０のいずれか１項に記載の配布センタ。
【請求項３３】

前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項２４から請求項３２のいずれか１項に記載の配布センタ。
【請求項３４】
前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、
を特徴とする、請求項２４から請求項３３のいずれか１項に記載の配布センタ。
【請求項３５】
前記配布センタはさらに、
前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、
を特徴とする、請求項２４から請求項３４のいずれか１項に記載の配布センタ。
【請求項３６】
前記コンテンツ位置情報生成部はさらに、
外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、
を特徴とする、請求項３５に記載の配布センタ。
【請求項３７】
前記コンテンツ位置情報生成部はさらに、
ランダムに前記コンテンツ位置情報を生成すること、
を特徴とする、請求項３５に記載の配布センタ。
【請求項３８】
コンテンツを実行、もしくは再生するコンテンツ実行方法であって、
前記コンテンツ実行方法は、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、
前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、
認証情報を検証するための検証情報を保持するステップと、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、
前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、
を含むことを特徴とするコンテンツ実行方法。
【請求項３９】
コンテンツを実行、もしくは再生するコンテンツ実行プログラムであって、
前記コンテンツ実行プログラムは、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、
前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、
認証情報を検証するための検証情報を保持するステップと、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、
前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、
を含むことを特徴とする実行プログラム。
【請求項４０】
請求項３９に記載のプログラムを記録した媒体。
【請求項４１】

コンテンツを実行、もしくは再生するコンテンツ実行装置の集積回路であって、
前記集積回路は、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、
認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、
前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする集積回路。
【請求項４２】
コンテンツを配布するコンテンツ配布方法であって、
前記コンテンツ配布方法は、
認証情報生成情報を保持するステップと、
前記コンテンツを入力するステップと、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、
前記コンテンツと、前記認証情報と、を配布するステップと、
を含むことを特徴とするコンテンツ配布方法。
【請求項４３】
コンテンツを配布する処理をコンピュータに実行させるプログラムであって、
前記コンテンツ配布プログラムは、
前記コンテンツを入力するステップと、
認証情報生成情報を保持するステップと、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、
前記コンテンツと、前記認証情報と、を配布するステップと、
を含むことを特徴とするコンピュータプログラム。
【請求項４４】
請求項４３に記載のプログラムを記録した媒体。
【請求項４５】
コンテンツを配布する配布センタにおける集積回路であって、
前記集積回路は、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、前記認証情報と、を配布する配布部と、

を備えることを特徴とする集積回路。
【請求項４６】
不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ取得し、それぞれの前記第一属性値を含む付加情報を生成する付加情報生成部と、
前記付加情報及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、前記付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、
前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第二属性値を取得し、それぞれの前記第二属性値と、前記付加情報に含まれる前記第二属性値の前記特定情報に対応するそれぞれの前記第一属性値を比較する付加情報検証部と、
前記認証情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項４７】
不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの当該部分コンテンツを取得し、一以上の前記当該部分コンテンツを含

むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、前記第二属性値を一以上含む第二属性値群を一以上生成する第二属性値群生成部と、
一以上の前記第二属性値群及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
前記コンテンツと、一以上の前記第一属性値及び一以上の前記第二属性値群を含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、
前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、それぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値と、前記付加情報に含まれる一以上の前記第二属性値とを比較する付加情報検証部と、
前記認証情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項４８】
不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値を一以上生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、それぞれの前記第二属性値を含む第二属性値群を生成する第二属性値郡生成部と、
前記第二属性値群及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び前記第二属性値群を含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、

前記コンテンツ位置情報を構成する前記特定情報の中から一部の前記特定情報を選択し、選択された一以上の前記特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、
前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値と、前記付加情報に含まれる一以上の前記第二属性値とを比較する付加情報検証部と、
前記認証情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項４９】
不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの当該部分コンテンツを取得し、一以上の前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証データを生成する検証データ生成部と、
一以上の前記検証対象データ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、
前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項５０】

不正コンテンツを検知する不正コンテンツ検知システムであって、
前記不正コンテンツ検知システムは、
可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値を一以上生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、それぞれの前記第二属性値を含む検証データを生成する検証データ生成部と、
前記検証データ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び前記検証データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、
前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。

【書類名】明細書
【発明の名称】不正コンテンツ検知システム
【技術分野】
【０００１】
本発明は不正なコンテンツを検知する技術に関するものである。
【背景技術】
【０００２】
近年、デジタルコンテンツの普及に伴い、著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる違法コンテンツの不正配布が社会問題となってきている。このコンテンツ不正配布の一つのケースとして、映画館等で上映される映画コンテンツを著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した動画コンテンツを光ディスクに記録し販売するというものが挙げられる。また別のケースとして、正規に販売されている片面２層ＤＶＤ－ＲＯＭディスク（最大８．５ギガバイト）に記録されているＤＶＤ－ＶＩＤＥＯ形式の映画コンテンツの画質を変換処理して４．７ギガバイト以下に収まるようにして、片面１層ＤＶＤ－Ｒディスク（最大４．７ギガバイト）に記録して販売するものも挙げられる。
【０００３】
上記のようなコンテンツ不正利用を防ぐ方法の従来技術としては、特許文献１に記載されている不正コンテンツ検知システムが知られている。この従来技術は、可搬媒体の中に、コンテンツデータの他に、複数の部分コンテンツデータに対応するハッシュ値と、複数の部分コンテンツデータを結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前と、コンテンツを再生している途中に、記録されたコンテンツデータが正規の著作権者によって記録されたものか、デジタル署名及びハッシュ値を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを正しく再生しない。これにより、不正なコンテンツの配布防止につながる。
【０００４】
ここでは、従来技術の詳細の一例を図７９を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。
初めに、正規の著作権者が、コンテンツデータと、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツをｃ個（ｃは２以上の自然数）のコンテンツブロック（図７９のコンテンツブロック　ＢＬＫ１・・・ＢＬＫｃに対応）に分割する。そして、一方向性関数を用いてコンテンツブロックＢＬＫ１のハッシュ値ＨＡＳＨ１を計算する。コンテンツブロックＢＬＫ２以降も同様にハッシュ値を計算し、それぞれのコンテンツブロックＢＬＫ２、・・・、ＢＬＫｃに対応するハッシュ値ＨＡＳＨ２、・・・、ＨＡＳＨｃを求める。そして、ｃ個のハッシュ値ＨＡＳＨ１、・・・、ＨＡＳＨｃを連結させたものをヘッダ情報ＨＥＡＤとする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報ＨＥＡＤのデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。
【０００５】
続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始する。その後、実行装置はコンテンツを再生しながら、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテン

ツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。

【０００６】

このような従来技術により、何らかの理由によりコンテンツが盗み出され、そのコンテンツを可搬媒体に記録して販売しようとしても、可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正なコンテンツ流通に対する対策が可能となる。

【特許文献１】米国特許第６４８０９６１号明細書

【特許文献２】特開２００２－２８１０１３号公報

【非特許文献１】「情報セキュリティ」宮地充子・菊池浩明編著　情報処理学会編集

【非特許文献２】「ＴＨＥ　ＡＲＴ　ＯＦ　ＣＯＭＰＵＴＥＲ　ＰＲＯＧＲＡＭＭＩＮＧ　　Ｖｏｌ．２　～　ＳＥＭＩＮＵＭＥＲＩＣＡＬ　ＡＬＧＯＲＩＴＨＭＳ」　ＤＯＮＡＬＤ　Ｅ．　ＫＮＵＴＨ　著、ＩＳＢＮ　０－２０１－０３８２２－６

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、前記従来技術では、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという課題を有していた。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【０００８】

本発明は、前記従来技術の課題を解決するもので、コンテンツ再生中の実行装置の処理負荷を軽減させた不正コンテンツ検知システムを提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、請求項１における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、前記コンテンツを、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、実行装置へ配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を取得する取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１０】

請求項２における発明は、請求項１に記載の不正コンテンツ検知システムであって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

請求項３における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１１】

請求項４における発明は、請求項３に記載の実行装置であって、前記取得部は、可搬媒体からデータを取得すること、を特徴とする。

請求項５における発明は、請求項３に記載の実行装置であって、前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、を特徴とする。

【００１２】

請求項６における発明は、請求項３から請求項５のいずれか１項に記載の実行装置であって、前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、を特徴とする。

請求項７における発明は、請求項３から請求項６のいずれか１項に記載の実行装置であって、前記実行装置は、さらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、を特徴とする。

【００１３】

請求項８における発明は、請求項７に記載の実行装置であって、前記実行装置は、さらに、前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、を特徴とする。

請求項９における発明は、請求項７または請求項８に記載の実行装置であって、前記実行装置は、さらに、デバイス鍵を保持するデバイス鍵格納部と、前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、前記取得部はさらに、前記暗号化鍵束を受信すること、を特徴とする。

【００１４】

請求項１０における発明は、請求項３から請求項９のいずれか１項に記載の実行装置であって、前記取得部は、ｍ個（ｍは２以上の自然数）の前記コンテンツ位置情報と、前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応するｍ個の前記認証情報の中から、ｂ組（ｂは１以上ｍ－１以下の自然数）の前記コンテンツ位置情報及び前記認証情報を取得し、前記検証部は、前記コンテンツ及びｍ個の前記コンテンツ位置情報を基に、ｍ個の前記代表部分コンテンツを取得し、ｍ個の前記代表部分コンテンツ及びｍ個の前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【００１５】

請求項１１における発明は、請求項１０に記載の実行装置であって、前記取得部は、ｍ組の前記コンテンツ位置情報及び前記認証情報の中から、ｂ組の前記コンテンツ位置情報及び前記認証情報をランダムに選択すること、を特徴とする。

請求項１２における発明は、請求項１０に記載の実行装置であって、前記取得部は、ｍ組の前記コンテンツ位置情報及び前記認証情報の中から、ｂ組の前記コンテンツ位置情報及び前記認証情報を順番に選択すること、を特徴とする。

【００１６】
請求項１３における発明は、請求項１０から請求項１２のいずれか１項に記載の実行装置であって、前記取得部において、ｂは１であること、を特徴とする。
請求項１４における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。
【００１７】
請求項１５における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。
請求項１６における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記検証情報は、デジタル署名方式の検証鍵であること、を特徴とする。
【００１８】
請求項１７における発明は、請求項３から請求項１６のいずれか１項に記載の実行装置であって、前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、前記取得部はさらに、前記検証情報識別子を受信し、前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。
【００１９】
請求項１８における発明は、請求項３から請求項１７のいずれか１項に記載の実行装置であって、前記取得部はさらに、前記検証情報を受信すること、を特徴とする。
請求項１９における発明は、請求項１６から請求項１８のいずれか１項に記載の実行装置であって、前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。
【００２０】
請求項２０における発明は、請求項１９に記載の実行装置であって、前記実行装置は、さらに、前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、を特徴とする。
請求項２１における発明は、請求項２０に記載の実行装置であって、前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、を特徴とする。
【００２１】
請求項２２における発明は、請求項２０または請求項２１に記載の実行装置であって、前記第二取得部と前記取得部は等しいこと、を特徴とする。
請求項２３における発明は、請求項３から請求項２２のいずれか１項に記載の実行装置であって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。
【００２２】
請求項２４における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を配布する配布部と、を備えることを特徴とする。

【００２３】
請求項２５における発明は、請求項２４に記載の配布センタであって、前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、を特徴とする。
請求項２６における発明は、請求項２４または請求項２５に記載の配布センタであって、前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、を特徴とする。
【００２４】
請求項２７における発明は、請求項２４から請求項２６のいずれか１項に記載の配布センタであって、前記配布センタはさらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、を特徴とする。
【００２５】
請求項２８における発明は、請求項２７に記載の配布センタであって、前記配布センタはさらに、一以上のデバイス鍵を保持する実行装置情報格納部と、前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、前記配布部はさらに、前記暗号化鍵束を配布すること、を特徴とする。
【００２６】
請求項２９における発明は、請求項２７または請求項２８に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、を特徴とする。
請求項３０における発明は、請求項２４から請求項２９のいずれか１項に記載の配布センタであって、前記コンテンツ位置情報格納部は、ｍ個（ｍは２以上の自然数）の前記コンテンツ位置情報及び前記コンテンツを保持し、前記認証情報生成部は、ｍ個の前記コンテンツ位置情報及び前記コンテンツを基に、ｍ個の前記代表部分コンテンツを取得し、ｍ個の前記代表部分コンテンツ及び前記認証情報生成情報を基に、ｍ個の認証情報を生成し、前記取得部は、前記コンテンツ位置情報と前記認証情報のｍ組を配布すること、を特徴とする。
【００２７】
請求項３１における発明は、請求項２４から請求項３０のいずれか１項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。
請求項３２における発明は、請求項２４から請求項３０のいずれか１項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。
【００２８】
請求項３３における発明は、請求項２４から請求項３２のいずれか１項に記載の配布センタであって、前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、を特徴とする。
請求項３４における発明は、請求項２４から請求項３３のいずれか１項に記載の配布センタであって、前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、を特徴とする。
【００２９】
請求項３５における発明は、請求項２４から請求項３４のいずれか１項に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、を特徴とする。
請求項３６における発明は、請求項３５に記載の配布センタであって、前記コンテンツ

位置情報生成部はさらに、外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、を特徴とする。

【００３０】

請求項３７における発明は、請求項３５に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに、ランダムに前記コンテンツ位置情報を生成すること、を特徴とする。

請求項３８における発明は、コンテンツを実行、もしくは再生するコンテンツ実行方法であって、前記コンテンツ実行方法は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、認証情報を検証するための検証情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、を含むことを特徴とする。

【００３１】

請求項３９における発明は、コンテンツを実行、もしくは再生するコンテンツ実行プログラムであって、前記コンテンツ実行プログラムは、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得するステップと、認証情報を検証するための検証情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定するステップと、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始するステップと、を含むことを特徴とする。

【００３２】

請求項４０における発明は、請求項３９に記載のプログラムを記録した媒体であることを特徴とする。

請求項４１における発明は、コンテンツを実行、もしくは再生するコンテンツ実行装置の集積回路であって、前記集積回路は、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツと前記コンテンツ位置情報を基に特定される前記代表部分コンテンツに対応する認証情報と、を外部から取得する取得部と、認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報及び前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定する検証部と、前記検証部で許可した場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００３３】

請求項４２における発明は、コンテンツを配布するコンテンツ配布方法であって、前記コンテンツ配布方法は、認証情報生成情報を保持するステップと、前記コンテンツを入力するステップと、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、前記コンテンツと、前記認証情報と、を配布するステップと、を含むことを特徴とする。

【００３４】

請求項４３における発明は、コンテンツを配布する処理をコンピュータに実行させるプ

ログラムであって、前記コンテンツ配布プログラムは、前記コンテンツを入力するステップと、認証情報生成情報を保持するステップと、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するステップと、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成するステップと、前記コンテンツと、前記認証情報と、を配布するステップと、を含むことを特徴とする。

【００３５】

請求項４４における発明は、請求項４３に記載のプログラムを記録した媒体であることを特徴とする。

請求項４５における発明は、コンテンツを配布する配布センタにおける集積回路であって、前記集積回路は、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である代表部分コンテンツを特定するコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記認証情報と、を配布する配布部と、を備えることを特徴とする。

【００３６】

請求項４６における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ取得し、それぞれの前記第一属性値を含む付加情報を生成する付加情報生成部と、前記付加情報及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、前記付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第二属性値を取得し、それぞれの前記第二属性値と、前記付加情報に含まれる前記第二属性値の前記特定情報に対応するそれぞれの前記第一属性値を比較する付加情報検証部と、前記認証情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００３７】

請求項４７における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対

応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの当該部分コンテンツを取得し、一以上の前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、前記第二属性値を一以上含む第二属性値群を一以上生成する第二属性値群生成部と、一以上の前記第二属性値群及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、一以上の前記第一属性値及び一以上の前記第二属性値群を含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、それぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値と、前記付加情報に含まれる一以上の前記第二属性値とを比較する付加情報検証部と、前記認証情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００３８】

請求項４８における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値を一以上生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、それぞれの前記第二属性値を含む第二属性値群を生成する第二属性値郡生成部と、前記第二属性値群及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び前記第二属性値群を含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記検証情報を基に、前記認証情報が前記付加情報の認証情報であるかどうか検証する認証情報検証部と、前記コンテンツ位置情報を構成する前記特定情報の中から一部の前記特定情報を選択し、選択された一以上の前記特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値と、前記付加情報に含まれる一以上の前記第二属性値とを比較する付加情報検証部と、前記認証

情報検証部及び前記付加情報検証部での検証結果が共に正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００３９】

請求項４９における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの当該部分コンテンツを取得し、一以上の前記当該部分コンテンツを含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証データを生成する検証データ生成部と、一以上の前記検証対象データ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００４０】

請求項５０における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる前記特定情報のそれぞれを基に、対応するそれぞれの当該部分コンテンツを取得し、前記当該部分コンテンツを含むデータに対する第一属性値を一以上生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、該第一属性値群に対する第二属性値をそれぞれ生成し、それぞれの前記第二属性値を含む検証データを生成する検証データ生成部と、前記検証データ及び前記認証情報生成情報を基に、認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び前記検証データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成する、特定情報選択部と、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する当該被選択部分コンテンツを取得し、前記当該被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記付加情報に含まれる一以上の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【発明の効果】

【００４１】

本発明の不正コンテンツ検知システムによれば、コンテンツを実行開始、もしくは再生開始する前にのみ、コンテンツが正規の著作権者により配布されたコンテンツ（正規コンテンツ）なのか、正規の著作権者以外により配布されたコンテンツ（不正コンテンツ）なのかを検証し、コンテンツの実行中、再生中にはその検証を行わないようにした。そうすることにより、不正コンテンツの実行、再生を制限（開始不許可など）することが出来るようになるとともに、従来技術に比べ、コンテンツ実行中、再生中の実行装置の処理負荷を軽減出来るようになった。

【００４２】

また、本発明の不正コンテンツ検知システムでは、さらに、実行装置がコンテンツを実行、再生開始する場合に、コンテンツに付随するコンテンツ位置情報に対応するコンテンツの一部分である、部分コンテンツの属性値（ハッシュ値）を検証のするようにした。この際、実施の形態１及び２における不正コンテンツ検知システムでは、コンテンツ位置情報を暗号化しておくことによって、不正者は、コンテンツのどの一部分が検証されるのか予測出来ないようになった。この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証するようにコンテンツ位置情報に記載されている場合に、実行、再生の制限（再生不許可など）が出来るようになった。なお、コンテンツ位置情報には、例えば、その部分のデータを変えてしまうとコンテンツ全体に影響を与えるようなコンテンツの特徴点（例えば、ＭＰＥＧデータにおけるＩピクチャなど）を選択すると効果的となる。

【００４３】

実施の形態２及び３及び４における不正コンテンツ検知システムでは、実行装置が同じコンテンツを実行、再生する場合にも、コンテンツの中の毎回異なる一部分の部分コンテンツの属性値（ハッシュ値）を検証するようにした。これにより、不正者は、次にコンテンツのどの一部分が検証されるのか予測出来ないようになった。この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、ある確率（実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証する場合）で実行、再生の制限（再生不許可など）が出来るようになった。

【００４４】

このことにより、コンテンツの中の全部もしくは一部分を、不正なコンテンツに差し替えられるような攻撃を防ぐことが出来、抑止力となる。これは、コンテンツデータとともに、そのコンテンツデータ全体に対する属性値（ハッシュ値）１つと、その属性値（ハッシュ値）に対するデジタル署名と、を記録した可搬媒体を配布する自明な方式に比べても優位性を持つ。何故なら、自明な方式の場合コンテンツデータ全体に対する属性値（ハッシュ値）を計算しなくてはならないため、コンテンツの実行、再生開始前の処理に時間がかかっていた。しかし、本発明の不正コンテンツ検知システムによれば、コンテンツの実行、再生開始前には、コンテンツデータの中の一部分、もしくは毎回異なる一部分の部分

コンテンツの属性値（ハッシュ値）だけを計算すれば良いので、自明な方式に比べ、処理時間を短縮することが出来る。
【発明を実施するための最良の形態】
【００４５】
以下本発明の実施の形態について、図面を参照しながら説明する。
（実施の形態１）
図１は、本発明の実施の形態１における不正コンテンツ検知システムの構成図である。図１において、配布センタ１０は外部からコンテンツＣＮＴを受け取り、後述する実行装置１２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体１１に記録するものであり、可搬媒体１１は実行装置１２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置１２は可搬媒体１１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。
【００４６】
不正コンテンツ検知システム１は、配布センタ１０（正規のコンテンツ提供者、著作権者）が、ＤＶＤ－ＲＯＭ等の可搬媒体１１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、コンテンツＣＮＴを基に生成されるヘッダ情報ＨＥＡＤのデジタル署名である認証情報ＡＵＴＨを、各実行装置１２へ配布する。各実行装置１２は、暗号化コンテンツＥＮＣＣＮＴを復号化してコンテンツＣＮＴを取得し、認証情報ＡＵＴＨが配布センタ１０によるヘッダ情報ＨＥＡＤの正規のデジタル署名であることと、ヘッダ情報ＨＥＡＤがコンテンツＣＮＴを基に生成されたものであることを確認し、コンテンツＣＮＴを実行開始する。
【００４７】
以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム１の詳細について説明を行う。
＜不正コンテンツ検知システム１の構成＞
不正コンテンツ検知システム１は、図１に示すように、配布センタ１０と、可搬媒体１１と、ｎ個の実行装置１２（ｎは１以上の自然数）から構成される。
【００４８】
以下に、これらの構成要素について、詳細に説明する。まず、配布センタ１０の構成と動作について述べ、続いて可搬媒体１１の構成について述べ、最後に実行装置１２の構成と動作について述べる。
＜配布センタ１０の構成＞
配布センタ１０は、図２に示すように、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、コンテンツ位置情報生成部１００５、ヘッダ情報生成部１００６、認証情報生成情報格納部１００７、認証情報生成部１００８、暗号化部１００９、配布部１０１０から構成される。
【００４９】
（１）入力部１００１
入力部１００１は、外部からコンテンツＣＮＴを入力出来るものである。入力部１００１は、例えば、可搬媒体であるＤＶＤ－ＲＯＭ等からコンテンツＣＮＴを読み取る機能を有する。外部から入力されるコンテンツＣＮＴは、例えば図３で示すように、ｃ個の部分コンテンツＣＮＴ―１、・・・、ＣＮＴ―ｃから構成されているとする。また、それぞれの部分コンテンツは、特定情報によって特定可能であるとする。この特定情報は、例えば、部分コンテンツの先頭を表す物理アドレスやセクタ情報、サイズ、コンテンツの先頭からの経過時間などであるが、部分コンテンツを特定可能な情報であれば、どのような情報でも良く、さらには、上記情報を組み合わせた情報であっても良い。さらに、コンテンツＣＮＴ（部分コンテンツＣＮＴ―１、・・・、ＣＮＴ―ｃ）は、実行装置１２で実行可能なフォーマット形式であって、例えば、ＭＰＥＧフォーマットによる動画データやＭＰ３フォーマットによる音声データなどである。外部からコンテンツＣＮＴが入力された場合、そのコンテンツＣＮＴをコンテンツ鍵生成部１００２へ出力する。例えば、ｃは１００

０００００であるが、ｃは１以上の自然数であればどのような値でも良い。

【００５０】

（２）コンテンツ鍵生成部１００２

コンテンツ鍵生成部１００２は、入力部１００１からコンテンツＣＮＴが入力された場合、コンテンツ鍵ＣＫを生成する。コンテンツ鍵ＣＫを生成する方法としては、例えば、乱数を用いてランダムに生成する方法などがある。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部１００４へ出力する。なお、コンテンツ鍵ＣＫはコンテンツＣＮＴ、及び、コンテンツ位置情報ＰＯＳを暗号化、復号化するための鍵であり、暗号化部１００９及び実行装置１２のコンテンツ位置情報取得部１２４及び部分復号化部１２７で使用される。

【００５１】

（３）実行装置情報格納部１００３

実行装置情報格納部１００３は、複数の実行装置１２に与えられる鍵情報を保持するものである。図４は、実行装置情報格納部１００３の一例を示しており、装置識別子ＡＩＤ１に対応付けられたデバイス鍵ＤＫ１と、装置識別子ＡＩＤ２に対応付けられたデバイス鍵ＤＫ２と、・・・、装置識別子ＡＩＤｎに対応付けられたデバイス鍵ＤＫｎを保持している状態を示している。ここで、装置識別子ＡＩＤ１、・・・、ＡＩＤｎのそれぞれは、複数の実行装置１２のいずれかに対応付けられており、デバイス鍵ＤＫ１、・・・、ＤＫｎのそれぞれは、対応する実行装置１２のデバイス鍵格納部１２２に格納されている鍵である。なお、デバイス鍵ＤＫ１、・・・、ＤＫｎはコンテンツ鍵ＣＫを暗号化、復号化するための鍵であり、暗号化鍵束生成部１００４及びコンテンツ鍵取得部１２３で用いられる。

【００５２】

（４）暗号化鍵束生成部１００４

暗号化鍵束生成部１００４は、コンテンツ鍵生成部１００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴが入力された場合、実行装置情報格納部１００３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成するものである。暗号化鍵束ＫＢは、各実行装置１２がその暗号化鍵束ＫＢと自身の保持する鍵を用いてコンテンツ鍵ＣＫが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置１２はそれぞれ、装置識別子とデバイス鍵の一組をいずれか保持しており、情報格納部１００３には、図４のように、実行装置１２が保持する装置識別子とデバイス鍵の全ての組が格納されているとする。そのような場合、暗号化鍵束ＫＢは例えば以下のように生成される。実行装置情報格納部１００３から装置識別子ＡＩＤ１と対応するデバイス鍵ＤＫ１を取得する。そして、デバイス鍵ＤＫ１を基にコンテンツ鍵ＣＫを暗号化し、暗号化コンテンツ鍵ＥＮＣＣＫ１を生成し、装置識別子ＡＩＤ１に対応付ける。そして、他の装置識別子とデバイス鍵に対しても同様の処理を行い、暗号化コンテンツ鍵ＥＮＣＣＫ２、・・・、ＥＮＣＣＫｎを生成し、装置識別子ＡＩＤ２、・・・、ＡＩＤｎに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵をｎ組含む、図５のような暗号化鍵束ＫＢを生成する。このような暗号化鍵束ＫＢの構成にすることによって、各実行装置１２はその暗号化鍵束ＫＢと自身の保持するデバイス鍵を用いてコンテンツ鍵ＣＫが取得出来るようになる。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部１００５に出力する。なお、特許文献２などに記載の方法を用いることで、暗号化鍵束ＫＢの中の暗号化コンテンツ鍵の数を減らすことや、ある特定の実行装置では正しいコンテンツ鍵を取得出来ないようにして、実行装置を無効化することも出来る。また、暗号化鍵束生成部１００４で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）方式などであり、実行装置１２のコンテンツ鍵取得部１２３と同じ暗号アルゴリズムを用いる。

【００５３】

（５）コンテンツ位置情報生成部１００５

コンテンツ位置情報生成部１００５は、暗号化鍵束生成部１００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、まずコンテンツＣＮＴを構成するｃ個の部分コンテンツＣＮＴ－１、・・・、ＣＮＴ－ｃの中から、一つの部分コンテンツを選択し、それを代表部分コンテンツＰ１－ＣＮＴとする。ここでは、図６に例として、部分コンテンツＣＮＴ－３を代表部分コンテンツＰ１－ＣＮＴとした場合について示している。このｃ個の部分コンテンツＣＮＴ－１、・・・、ＣＮＴ－ｃの中から代表部分コンテンツを選択する方法としては、例えば、以下で説明するような３つの方法がある。

【００５４】

一つ目の方法は、コンテンツデータのある特徴点（例えば、ＭＰＥＧ動画データにおけるＩピクチャやＧＯＰなど）を自動的に選択する方法である。二つ目は、乱数を用いてランダムに自動的に選択する方法である。この二つの方法においては、コンテンツ位置情報生成部１００５は、図２で示すような外部から要求情報ＲＥＱを受け取る機能や外部へコンテンツを出力する機能は必要はない。なお、特徴点（ＩピクチャやＧＯＰなど）の全てを必ずしも選択する必要はなく、特徴点の一部のみを選択するようにしても良い。そして三つ目は、コンテンツ位置情報生成部１００５は外部へコンテンツＣＮＴの中の部分コンテンツを順番に実行する機能を有し、外部から（例えばユーザが）要求信号ＲＥＱをコンテンツ位置情報生成部１００５へ入力したときに実行している部分コンテンツを代表部分コンテンツとするものである。この三つ目の方法は、コンテンツ位置情報生成部１００５がディスプレイやキーボードなどの入出力装置を備えることによって実現出来る。

【００５５】

そして、その代表部分コンテンツＰ１－ＣＮＴを指し示す特定情報をＡＤＤＲ１とする。そして、続けて、ｋ－１個の代表部分コンテンツＰ２－ＣＮＴ、・・・、Ｐｋ－ＣＮＴを選択し、その代表部分コンテンツに対応する特定情報をＡＤＤＲ２、・・・、ＡＤＤＲｋとする（図６参照）。そして、その代表部分コンテンツと特定情報のｋ組｛Ｐ１－ＣＮＴ、ＡＤＤＲ１｝、｛Ｐ２－ＣＮＴ、ＡＤＤＲ２｝、・・・、｛Ｐｋ－ＣＮＴ、ＡＤＤＲｋ｝を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫと併せて、ヘッダ情報生成部１００６へ出力する。ｋは例えば２０であるが、２０以外であっても、１以上の自然数であればどのような値でも良く、例えば、代表部分コンテンツと特定情報が一組であってもよい。また、代表部分コンテンツのサイズは、例えば６４キロバイトであるが、６４キロバイトに限らず、どのようなサイズであっても良く、さらには、代表部分コンテンツ毎に異なるサイズであっても良い。例えば、代表部分コンテンツＰ１－ＣＮＴが１０キロバイトで、代表部分コンテンツＰｋ－ＣＮＴが２キロバイトであっても良い。また、選択する部分コンテンツは、コンテンツＣＮＴに応じて変えても良い。

【００５６】

（６）ヘッダ情報生成部１００６

ヘッダ情報生成部１００６は、コンテンツ位置情報生成部１００５から、代表部分コンテンツと特定情報のｋ組｛Ｐ１－ＣＮＴ、ＡＤＤＲ１｝、｛Ｐ２－ＣＮＴ、ＡＤＤＲ２｝、・・・、｛Ｐｋ－ＣＮＴ、ＡＤＤＲｋ｝と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤを生成する。まず、代表部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。特定情報識別子を生成する方法としては、自然数を順番に割り当てていく（１、２、・・・、ｋ）方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した特定情報識別子をそれぞれ、ＡＤＤＲＩＤ１、ＡＤＤＲＩＤ２、・・・ＡＤＤＲＩＤｋとし、次のように特定情報識別子と代表部分コンテンツと特定情報とが対応しているとする。｛ＡＤＤＲＩＤ１、Ｐ１－ＣＮＴ、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ２、Ｐ２－ＣＮＴ、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤｋ、Ｐｋ－ＣＮＴ、ＡＤＤＲｋ｝。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を計算する。代表部分コンテンツのハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１（Ｓｅｃｕｒｅ

Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ－１）アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ　－　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）などがあり、実行装置１２のヘッダ情報検証部１２８で用いる方法と同じものを用いる。ここで、各組に対して計算したハッシュ値をそれぞれ、ＨＡＳＨ１、ＨＡＳＨ２、・・・ＨＡＳＨｋとし、次のように特定情報識別子と代表部分コンテンツと特定情報とハッシュ値が対応しているとする。｛ＡＤＤＲＩＤ１、Ｐ１－ＣＮＴ、ＡＤＤＲ１、ＨＡＳＨ１｝、｛ＡＤＤＲＩＤ２、Ｐ２－ＣＮＴ、ＡＤＤＲ２、ＨＡＳＨ２｝、・・・、｛ＡＤＤＲＩＤｋ、Ｐｋ－ＣＮＴ、ＡＤＤＲｋ、ＨＡＳＨｋ｝。そして、その中から特定情報識別子と特定情報だけを抽出し、図７で示すような、特定情報識別子と特定情報とを含むコンテンツ位置情報ＰＯＳ＝｛ＡＤＤＲＩＤ１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ２、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤｋ、ＡＤＤＲｋ｝を生成する。また、特定情報識別子とハッシュ値だけを抽出し、図８で示すような、特定情報識別子とハッシュ値とを含むヘッダ情報ＨＥＡＤ＝｛ＡＤＤＲＩＤ１、ＨＡＳＨ１｝、｛ＡＤＤＲＩＤ２、ＨＡＳＨ２｝、・・・、｛ＡＤＤＲＩＤｋ、ＨＡＳＨｋ｝を生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部１００８へ出力する。

【００５７】

（７）認証情報生成情報格納部１００７

認証情報生成情報格納部１００７は、ヘッダ情報ＨＥＡＤの認証情報ＡＵＴＨを生成するための、認証情報生成情報ＧＥＮＡＵＴＨを保持するものである。この認証情報生成Ｘ情報ＧＥＮＡＵＴＨは、例えば、デジタル署名の署名生成鍵である。認証情報生成情報ＧＥＮＡＵＴＨに対応する検証情報ＶＥＲは、実行装置１２の検証情報格納部１２５に格納されている。この検証情報ＶＥＲは、例えば、デジタル署名の署名検証鍵である。また、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ（Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）方式などである。

【００５８】

（８）認証情報生成部１００８

認証情報生成部１００８は、ヘッダ情報生成部１００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値に対する認証情報ＡＵＴＨを生成する。まず、認証情報生成情報格納部１００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤと認証情報生成情報ＧＥＮＡＵＴＨを用いて、ヘッダ情報ＨＥＡＤの認証情報ＡＵＴＨを生成する。なお、認証情報ＡＵＴＨの生成方法の一例は、デジタル署名アルゴリズムであり、ｋ個のハッシュ値ＨＡＳＨ１、・・・、ＨＡＳＨｋを連結した値に対するデジタル署名である。具体的には例えば非特許文献１に記載のＤＳＡ方式などであり、実行装置１２の認証情報検証部１２６で用いるデジタル署名検証アルゴリズムと同じデジタル署名アルゴリズムを用いる。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部１００９へ出力する。

【００５９】

（９）暗号化部１００９

暗号化部１００９は、認証情報生成部１００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして暗号化コンテンツＥＮＣＣＮＴと暗号化コンテンツ位置情報ＥＮＣＰＯＳを生成する。まず、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。この暗号化コンテンツＥＮＣＣＮＴの生成方法としては、例えば、以下のような方法がある。まず、コンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ－１を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ－１を生成する。続いて、同じコンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ－２を暗号化

し、暗号化部分コンテンツＥＮＣＣＮＴ－２を生成する。これを繰り返して、図９で示すような暗号化部分コンテンツＥＮＣＣＮＴ－１、・・・、ＥＮＣＣＮＴ－ｃから構成される暗号化コンテンツを生成する。また、コンテンツ鍵ＣＫを基に、コンテンツ位置情報ＰＯＳを暗号化し、暗号化コンテンツ位置情報ＥＮＣＰＯＳを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを配布部１０１０へ出力する。なお、暗号化部１００９で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式などであり、実行装置１２のコンテンツ位置情報取得部１２４及び部分復号化部１２７と同じ暗号アルゴリズムを用いる。さらに、暗号化コンテンツＥＮＣＣＮＴの生成方法として、各部分コンテンツに対して、全て一つの同じコンテンツ鍵ＣＫで暗号化していたが、非特許文献１に記載のブロック暗号のモードを利用してもよい。例えば、ＣＢＣモードやＯＦＢ（Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ）モード、ＣＦＢ（Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ）モードでもよく、さらに、ある一定間隔毎にあるモード（例：ＣＢＣモード）の初期値を初期化するようにしたものでも良い。

【００６０】

（１０）配布部１０１０

配布部１０１０は、暗号化部１００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを可搬媒体１１へ記録するものである。

＜配布センタ１０の動作＞

以上で、配布センタ１０の構成について説明を行ったが、ここでは配布センタ１０の動作の一例について、図１０に示すフローチャートの処理を行う。なお、配布センタ１０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【００６１】

入力部１００１は、外部から入力されたコンテンツＣＮＴをコンテンツ鍵生成部１００２へ出力し、コンテンツ鍵生成部１００２は、コンテンツ鍵ＣＫを生成し、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部１００４へ出力する（ステップＳ１０１）。

暗号化鍵束生成部１００４は、コンテンツ鍵生成部１００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴを入力され、実行装置情報格納部１００３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部１００５に出力する（ステップＳ１０２）。

【００６２】

コンテンツ位置情報生成部１００５、暗号化鍵束生成部１００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫを入力され、ｋ個の代表部分コンテンツを選択し、そのｋ個の代表部分コンテンツに対応する特定情報を取得する。そして、その代表部分コンテンツと特定情報のｋ組を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとあわせて、ヘッダ情報生成部１００６へ出力する（ステップＳ１０３）。

【００６３】

ヘッダ情報生成部１００６は、コンテンツ位置情報生成部１００５から、代表部分コンテンツと特定情報のｋ組と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、代表部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を計算する。そして、その中から特定情報識別子と特定情報だけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報ＰＯＳと、特定情報識別子とハッシュ値とを含むヘッダ情報ＨＥＡＤを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部１００８へ出力する（ステップＳ１０４）。

【００６４】
認証情報生成部１００８は、ヘッダ情報生成部１００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、認証情報生成情報格納部１００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤと認証情報生成情報ＧＥＮＡＵＴＨとを用いて、ヘッダ情報ＨＥＡＤに対する認証情報ＡＵＴＨを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部１００９へ出力する（ステップＳ１０５）。
【００６５】
暗号化部１００９は、認証情報生成部１００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成し、同様にコンテンツ鍵ＣＫを基に、コンテンツ位置情報ＰＯＳを暗号化し、暗号化コンテンツ位置情報ＥＮＣＰＯＳを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを配布部１０１０へ出力する（ステップＳ１０６）。
【００６６】
配布部１０１０は、暗号化部１００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを可搬媒体１１へ記録する（ステップＳ１０７）。
以上が、不正コンテンツ検知システム１の構成要素である配布センタ１０の構成と動作である。続いて、可搬媒体１１の構成について説明を行う。
【００６７】
＜可搬媒体１１の構成＞
可搬媒体１１は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のような可搬媒体であり、図１１に示すように、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが配布センタ１０によって記録されているものとする。
【００６８】
以上が、不正コンテンツ検知システム１の構成要素である可搬媒体１１の構成である。続いて、実行装置１２の構成と動作について説明を行う。
＜実行装置１２の構成＞
実行装置１２は、図１２に示すように、取得部１２１、デバイス鍵格納部１２２、コンテンツ鍵取得部１２３、コンテンツ位置情報取得部１２４、検証情報格納部１２５、認証情報検証部１２６、部分復号化部１２７、ヘッダ情報検証部１２８、実行部１２９とから構成される。
【００６９】
（１）取得部１２１
取得部１２１は、可搬媒体１１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを受信する。そして、受信した暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ鍵取得部１２３へ出力する。
【００７０】
（２）デバイス鍵格納部１２２
デバイス鍵格納部１２２は、配布センタ１０の実行装置情報格納部１００３の中の鍵情報の一部を保持するものであり、このデバイス鍵格納部１２２に与えられる鍵情報と、暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫが取得出来るものである。例えば、実行装置情報格納部１００３が図３のような場合、デバイス鍵格納部１２２には、例として装置識別

子ＡＩＤｉとデバイス鍵Ｋｉ（ｉは１からｎのいずれか）が与えられる。
【００７１】
（３）コンテンツ鍵取得部１２３
コンテンツ鍵取得部１２３は、取得部１２１から暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、デバイス鍵格納部１２２に格納されている鍵情報及び暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫを取得する。例えば、暗号化鍵束ＫＢが図５のような場合で、デバイス鍵格納部１２２には装置識別子ＡＩＤｉとデバイス鍵ＤＫｉ（ｉは１からｎのいずれか）が与えられている場合、コンテンツ鍵取得部１２３はデバイス鍵格納部１２２から装置識別子ＡＩＤｉとデバイス鍵ＤＫｉを取得し、暗号化鍵束ＫＢの中から装置識別子ＡＩＤｉに対応する暗号化コンテンツ鍵ＥＮＣＣＫｉを取得し、デバイス鍵ＤＫｉを基に、暗号化コンテンツ鍵ＥＮＣＣＫｉを復号化することによって、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴをコンテンツ位置情報取得部１２４へ出力する。
【００７２】
（４）コンテンツ位置情報取得部１２４
コンテンツ位置情報取得部１２４は、コンテンツ鍵取得部１２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、コンテンツ鍵ＣＫを基に、暗号化コンテンツ位置情報ＥＮＣＰＯＳを復号化し、コンテンツ位置情報ＰＯＳを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを認証情報検証部１２６へ出力する。
【００７３】
（５）検証情報格納部１２５
検証情報格納部１２５は、ヘッダ情報ＨＥＡＤに対する認証情報ＡＵＴＨの正当性を検証するために必要な検証情報ＶＥＲを保持するものである。この検証情報ＶＥＲに対応する認証情報生成情報ＧＥＮＡＵＴＨは、配布センタ１０の認証情報生成情報格納部１００７に格納されている。例えば、検証情報ＶＥＲはデジタル署名アルゴリズムの署名検証鍵である。
【００７４】
（６）認証情報検証部１２６
認証情報検証部１２６は、コンテンツ位置情報取得部１２４からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、認証情報ＡＵＴＨが発行センタ１０によるヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値の正しい認証情報であるかを検証する。例えば、以下のような流れで検証する。まず、検証情報格納部１２５に格納されている検証情報ＶＥＲを取得する。そして、デジタル署名検証アルゴリズムを用いて、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値の正しいデジタル署名であるかを検証する。例えば、認証情報ＡＵＴＨが、ｋ個のハッシュ値ＨＡＳＨ１、・・・、ＨＡＳＨｋを連結した値に対する正規のデジタル署名であるかどうか検証する。このデジタル署名検証アルゴリズムは、配布センタ１０の認証情報生成部１００８で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。認証情報検証部１２６は、認証情報ＡＵＴＨが発行センタ１０によるヘッダ情報ＨＥＡＤの正しいデジタル署名である場合にのみ、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴを部分復号化部１２７へ出力する。
【００７５】
（７）部分復号化部１２７
部分復号化部１２７は、認証情報検証部１２６からコンテンツ鍵ＣＫとヘッダ情報ＨＥ

ＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、以下の処理を行う。まず、コンテンツ位置情報ＰＯＳの一組目の特定情報識別子ＡＤＤＲＩＤ１と特定情報ＡＤＤＲ１を抽出する。そして、暗号化コンテンツＥＮＣＣＮＴの中から特定情報ＡＤＤＲ１が特定する暗号化代表部分コンテンツＥＮＣＰ１－ＣＮＴを取得し、コンテンツ鍵ＣＫを基に復号化を行い、代表部分コンテンツＰ１－ＣＮＴを取得する。続いて、コンテンツ位置情報ＰＯＳの二組目以降の特定情報識別子ＡＤＤＲＩＤ２、・・・、ＡＤＤＲＩＤｋと特定情報ＡＤＤＲ２、・・・、ＡＤＤＲｋとを同様に抽出し、代表部分コンテンツＰ２－ＣＮＴ、・・・、Ｐｋ－ＣＮＴを取得する。そして、ヘッダ情報ＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、抽出されたｋ組の特定情報識別子ＡＤＤＲＩＤ１、・・・、ＡＤＤＲＩＤｋと代表部分コンテンツＰ１－ＣＮＴ、・・・、Ｐｋ－ＣＮＴと、コンテンツ鍵ＣＫと、をヘッダ情報検証部１２８へ出力する。なお、部分復号化部１２７で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式などであり、配布センタ１０の暗号化部１００９と同じ暗号アルゴリズムを用いる。

【００７６】

（８）ヘッダ情報検証部１２８

ヘッダ情報検証部１２８は、部分復号化部１２７からヘッダ情報ＨＥＡＤとコンテンツＣＮＴとｋ組の特定情報識別子ＡＤＤＲＩＤ１、・・・、ＡＤＤＲＩＤｋと代表部分コンテンツＰ１－ＣＮＴ、・・・、Ｐｋ－ＣＮＴと、コンテンツ鍵ＣＫと、が入力された場合、まず、一組目の特定情報識別子ＡＤＤＲＩＤ１と代表部分コンテンツＰ１－ＣＮＴに対して、以下の処理を行う。最初に、代表部分コンテンツＰ１－ＣＮＴに対して、そのハッシュ値Ｘを計算する。代表部分コンテンツのハッシュ値を求める方法としては、例えば、一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、配布センタ１０のヘッダ情報生成部１００８で用いる方法と同じものを用いる。そして、ヘッダ情報ＨＥＡＤの中の特定情報識別子ＡＤＤＲＩＤ１に対応するハッシュ値ＨＡＳＨ１と計算されたハッシュ値Ｘが等しいかどうか確認する。もし、同じ値であれば、二組目以降の特定情報識別子と代表部分コンテンツに対しても、同様にしてハッシュ値を計算し、ヘッダ情報ＨＥＡＤの中の対応する特定情報識別子のハッシュ値と比較する。ここで、全組のハッシュ値が等しかった場合にのみ、ヘッダ情報検証部１２８は実行部１２９へ暗号化コンテンツＥＮＣＣＮＴとコンテンツ鍵ＣＫと、を出力する。

【００７７】

（９）実行部１２９

実行部１２９は、ヘッダ情報検証部１２８から入力された暗号化コンテンツＥＮＣＣＮＴの中のｃ個の暗号化部分コンテンツＥＮＣＣＮＴ－１、・・・、ＥＮＣＣＮＴ－ｃを、コンテンツ鍵ＣＫを基に逐次復号化を行って部分コンテンツを取得し、逐次その部分コンテンツを実行するものであり、例えばディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生する、別の可搬媒体や記録媒体にコンテンツデータを出力する、コンテンツデータを紙などに印刷するなどがある

＜実行装置１２の動作＞

以上で、実行装置１２の構成について説明を行ったが、ここで実行装置１２の動作について、図１３に示すフローチャートを用いて説明する。なお、実行装置１２の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【００７８】

取得部１２１は、可搬媒体１１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ鍵取得部１２３へ出力する。そして、コンテンツ鍵取得部１２３は、入力された暗号化鍵束ＫＢ及びデバイス鍵格納部１２２が保持している鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ位置情報取得部１２４へ出力する（ステップＳ

１２１）。

【００７９】

コンテンツ位置情報取得部１２４は、コンテンツ鍵取得部１２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを入力された場合、コンテンツ鍵ＣＫを基に暗号化コンテンツ位置情報ＥＮＣＰＯＳを復号化し、コンテンツ位置情報ＰＯＳを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを認証情報検証部１２６へ出力する（ステップＳ１２２）。

【００８０】

認証情報検証部１２６は、コンテンツ位置情報取得部１２４からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを入力された場合、検証情報格納部１２５に格納されている検証情報ＶＥＲを用いて、ヘッダ情報ＨＥＡＤに対する正しい認証情報ＡＵＴＨであるかを検証する（ステップＳ１２３）。

【００８１】

認証情報検証部１２６は、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する発行センタ１０の正しい認証情報である場合にのみ、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴを部分復号化部１２７へ出力し、ステップＳ１２５へ進む。もし、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する正しい認証情報ではない場合、処理を終了する（ステップＳ１２４）。

【００８２】

部分復号化部１２７は、認証情報検証部１２６からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとを入力される。そして、コンテンツ鍵ＣＫを基に、暗号化コンテンツＥＮＣＣＮＴの中のｋ個の特定情報のそれぞれに対する暗号化代表部分コンテンツをそれぞれ復号化し、ｋ個の代表部分コンテンツＰ１―ＣＮＴ、・・・、Ｐｋ―ＣＮＴを抽出する。そして、ヘッダ情報ＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、ｋ組の特定情報識別子ＡＤＤＲＩＤ１、・・・、ＡＤＤＲＩＤｋと代表部分コンテンツＰ１―ＣＮＴ、・・・、Ｐｋ―ＣＮＴと、コンテンツ鍵ＣＫと、をヘッダ情報検証部１２８へ出力する（ステップＳ１２５）。

【００８３】

ヘッダ情報検証部１２８は、部分復号化部１２７からヘッダ情報ＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、ｋ組の特定情報識別子ＡＤＤＲＩＤ１、・・・、ＡＤＤＲＩＤｋと代表部分コンテンツＰ１―ＣＮＴ、・・・、Ｐｋ―ＣＮＴと、コンテンツ鍵ＣＫと、を入力される。そして、各組の代表部分コンテンツに対して、そのハッシュ値を計算する（ステップＳ１２６）。

【００８４】

ヘッダ情報検証部１２８は、計算したハッシュ値と、ヘッダ情報ＨＥＡＤの中の特定情報識別子に対応するハッシュ値とが等しいかどうか確認し、もし、全てのハッシュ値が同じ値であれば、ヘッダ情報検証部１２８は実行部１２９へ暗号化コンテンツＥＮＣＣＮＴとコンテンツ鍵ＣＫを出力し、ステップＳ１２８へ進む。もし、一つでも値が一致しなければ、処理を終了する（ステップＳ１２７）。

【００８５】

実行部１２９は、ヘッダ情報検証部１２８から受け取った暗号化コンテンツＥＮＣＣＮＴの中の暗号化部分コンテンツを、コンテンツ鍵を用いて逐次復号化し、その部分コンテンツを実行する（ステップＳ１２８）。

以上が、不正コンテンツ検知システム１の構成要素である実行装置１２の構成と動作である。尚、コンテンツ鍵取得部１２３、コンテンツ位置情報取得部１２４、認証情報検証部１２６等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化

されても良い。
【００８６】
ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。
また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。
【００８７】
さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。
＜不正コンテンツ検知システム１の効果＞
以上、不正コンテンツ検知システム１について実施の形態に基づいて説明したが、この不正コンテンツ検知システム１においては、配布センタ１０が、暗号化されたコンテンツＣＮＴとともに、コンテンツＣＮＴの中の、コンテンツ位置情報ＰＯＳが特定する代表部分コンテンツに対応するヘッダ情報ＨＥＡＤ、及び、ヘッダ情報に対する認証情報ＡＵＴＨ（例えばデジタル署名）、及び、暗号化されたコンテンツ位置情報ＰＯＳである暗号化コンテンツ位置情報ＥＮＣＰＯＳを可搬媒体１１に記録するようにして、実行装置１２が、コンテンツＣＮＴの実行開始前に、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する正規の認証情報（例えばデジタル署名）であるか検証するとともに、暗号化コンテンツ位置情報ＥＮＣＰＯＳを復号化してコンテンツ位置情報ＰＯＳを取得し、ヘッダ情報ＨＥＡＤがコンテンツＣＮＴの中のコンテンツ位置情報ＰＯＳが特定する代表部分コンテンツに対応する正規のヘッダ情報であるかを検証し、共に正当であると検証された場合にのみ、コンテンツＣＮＴの実行を開始するようにした。そうすることにより、実行装置１２は、不正な認証情報ＡＵＴＨもしくはヘッダ情報ＨＥＡＤもしくはコンテンツＣＮＴが記録された可搬媒体１１のコンテンツＣＮＴは実行開始しないようになり、不正コンテンツの配布を防止することが出来るようになった。
【００８８】
さらに、コンテンツ位置情報ＰＯＳは暗号化されて可搬媒体１１に記録されているため、不正者がコンテンツＣＮＴの中のコンテンツ位置情報ＰＯＳが特定する代表部分コンテンツのみを差し替えようとする攻撃が適用不可能となる。また、実行装置１２は、認証情報ＡＵＴＨの正当性の検証を、コンテンツＣＮＴを実行開始する前に全て行うため、コンテンツＣＮＴの実行中の特別な処理が必要なくなり、コンテンツＣＮＴの実行中の処理負荷が軽減されるという効果を有する。
【００８９】
（実施の形態２）
図１４は、本発明の実施の形態２の不正コンテンツ検知システムの構成図である。実施の形態２においては、実施の形態１と同様に、配布センタ２０は外部からコンテンツＣＮＴを受け取り、後述する実行装置２２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体２１に記録するものであり、可搬媒体２１はコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置２２は可搬媒体２１に記録されている情報を基にコンテンツＣＮＴを実行するものである。
【００９０】
実施の形態１では、可搬媒体１１はヘッダ情報と暗号化コンテンツ位置情報と認証情報とを１種類ずつ含んでいたが、実施の形態２での可搬媒体２１では、ヘッダ情報と暗号化コンテンツ位置情報と認証情報とをそれぞれ複数種類含んでいる点が異なる。そして、各実行装置２２は、可搬媒体２１からその一部のヘッダ情報と暗号化コンテンツ位置情報と認証情報とを選択し、その選択したヘッダ情報と暗号化コンテンツ位置情報と認証情報のみを検証する点が実施の形態１と異なる。

【００９１】
以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム２の詳細について説明を行う。
＜不正コンテンツ検知システム２の構成＞
不正コンテンツ検知システム２は、図１４に示すように、配布センタ２０と、可搬媒体２１と、複数の実行装置２２から構成される。
【００９２】
以下に、これらの構成要素について、詳細に説明する。まず、配布センタ２０の構成と動作について述べ、続いて可搬媒体２１の構成について述べ、最後に実行装置２２の構成と動作について述べる。
＜配布センタ２０の構成＞
配布センタ２０は、図１５に示すように、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、コンテンツ位置情報生成部２００５、ヘッダ情報生成部２００６、認証情報生成情報格納部１００７、認証情報生成部２００８、暗号化部２００９、配布部２０１０から構成される。なお、入力部１００１、コンテンツ鍵生成部１００２、実行装置情報格納部１００３、暗号化鍵束生成部１００４、認証情報生成情報格納部１００７については、実施の形態１の配布センタ１０と同じ構成要素であるため、説明を省略する。
【００９３】
（１）コンテンツ位置情報生成部２００５
コンテンツ位置情報生成部２００５において、実施の形態１のコンテンツ位置情報生成部１００５と異なる点についてのみ説明する。コンテンツ位置情報生成部１００５では、ｋ個の代表部分コンテンツとｋ個の特定情報をそれぞれ１種類のみ作成していたが、コンテンツ位置情報生成部２００５においては、ｋ個の代表部分コンテンツとｋ個の特定情報をそれぞれｍ種類作成する点が異なる。そのｍ種類をそれぞれ｛｛Ｐ１－１－ＣＮＴ、ＡＤＤＲ１－１｝、｛Ｐ２－１－ＣＮＴ、ＡＤＤＲ２－１｝、・・・、｛Ｐｋ－１－ＣＮＴ、ＡＤＤＲｋ－１｝｝、｛｛Ｐ１－２－ＣＮＴ、ＡＤＤＲ１－２｝、｛Ｐ２－２－ＣＮＴ、ＡＤＤＲ２－２｝、・・・、｛Ｐｋ－２－ＣＮＴ、ＡＤＤＲｋ－２｝｝、・・・、｛｛Ｐ１－ｍ－ＣＮＴ、ＡＤＤＲ１－ｍ｝、｛Ｐ２－ｍ－ＣＮＴ、ＡＤＤＲ２－ｍ｝、・・・、｛Ｐｋ－ｍ－ＣＮＴ、ＡＤＤＲｋ－ｍ｝｝とする。そして、ｍ種類それぞれに対して、ヘッダ識別子ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍを生成し、それぞれに対応づける。ヘッダ識別子を生成する方法としては、自然数を順番に割り当てていく（１、２、３、・・・、ｍ）方法や、乱数を用いる方法などがある。その状態を、｛ＨＥＡＤＩＤ１、｛Ｐ１－１－ＣＮＴ、ＡＤＤＲ１－１｝、｛Ｐ２－１－ＣＮＴ、ＡＤＤＲ２－１｝、・・・、｛Ｐｋ－１－ＣＮＴ、ＡＤＤＲｋ－１｝｝、｛ＨＥＡＤＩＤ２、｛Ｐ１－２－ＣＮＴ、ＡＤＤＲ１－２｝、｛Ｐ２－２－ＣＮＴ、ＡＤＤＲ２－２｝、・・・、｛Ｐｋ－２－ＣＮＴ、ＡＤＤＲｋ－２｝｝、・・・、｛ＨＥＡＤＩＤｍ、｛Ｐ１－ｍ－ＣＮＴ、ＡＤＤＲ１－ｍ｝、｛Ｐ２－ｍ－ＣＮＴ、ＡＤＤＲ２－ｍ｝、・・・、｛Ｐｋ－ｍ－ＣＮＴ、ＡＤＤＲｋ－ｍ｝｝とする。そして、ヘッダ識別子とｋ個の代表部分コンテンツとｋ個の特定情報をそれぞれｍ種類と、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとをあわせて、ヘッダ情報生成部２００６へ出力する。ｍは例えば１０であるが、２以上の自然数であればどのような値でも良い。
【００９４】
（２）ヘッダ情報生成部２００６
ヘッダ情報生成部２００６において、実施の形態１のヘッダ情報生成部１００６と異なる点についてのみ説明する。ヘッダ情報生成部１００６では、ｋ個の代表部分コンテンツとｋ個の特定情報の１種類に対してのみヘッダ情報を作成していたが、ヘッダ情報生成部２００６においては、ｋ個のヘッダ情報識別子とｋ個の代表部分コンテンツとｋ個の特定情報のｍ種類それぞれに対して、ヘッダ情報を作成（ヘッダ情報をｍ個）する点が異なる。それぞれのヘッダ情報を作成する方法は、実施の形態１のヘッダ情報生成部１００６と

同じ方法である。まず実施の形態１のヘッダ情報生成部１００６と同様に、各代表部分コンテンツに対して、特定情報識別子とハッシュ値を作成した結果を以下のように表記する。｛ＨＥＡＤＩＤ１、｛ＡＤＤＲＩＤ１－１、Ｐ１－１－ＣＮＴ、ＡＤＤＲ１－１、ＨＡＳＨ１－１｝、｛ＡＤＤＲＩＤ２－１、Ｐ２－１－ＣＮＴ、ＡＤＤＲ２－１、ＨＡＳＨ２－１｝、・・・、｛ＡＤＤＲＩＤｋ－１、Ｐｋ－１－ＣＮＴ、ＡＤＤＲｋ－１、ＨＡＳＨｋ－１｝｝、｛ＨＥＡＤＩＤ２、｛ＡＤＤＲＩＤ１－２、Ｐ１－２－ＣＮＴ、ＡＤＤＲ１－２、ＨＡＳＨ１－２｝、｛ＡＤＤＲＩＤ２－２、Ｐ２－２－ＣＮＴ、ＡＤＤＲ２－２、ＨＡＳＨ２－２｝、・・・、｛ＡＤＤＲＩＤｋ－２、Ｐｋ－２－ＣＮＴ、ＡＤＤＲｋ－２、ＨＡＳＨｋ－２｝｝、・・・、｛ＨＥＡＤＩＤｍ、｛ＡＤＤＲＩＤ１－ｍ、Ｐ１－ｍ－ＣＮＴ、ＡＤＤＲ１－ｍ、ＨＡＳＨ１－ｍ｝、｛ＡＤＤＲＩＤ２－ｍ、Ｐ２－ｍ－ＣＮＴ、ＡＤＤＲ２－ｍ、ＨＡＳＨ２－ｍ｝、・・・、｛ＡＤＤＲＩＤｋ－ｍ、Ｐｋ－ｍ－ＣＮＴ、ＡＤＤＲｋ－ｍ、ＨＡＳＨｋ－ｍ｝｝。そして、実施の形態１のヘッダ情報生成部１００６と同様の処理に、その中から、ヘッダ識別子と特定情報識別子と特定情報だけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報をｍ種類（ＰＯＳ－１、・・・、ＰＯＳ－ｍ）それぞれヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）と対応づけて生成する。また、同様にその中から、ヘッダ識別子と特定情報識別子とハッシュ値だけを抽出し、特定情報識別子とハッシュ値とを含むｍ種類のヘッダ情報（ＨＥＡＤ－１、・・・、ＨＥＡＤ－ｍ）をヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）と対応付けて生成する。そして、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳ１、・・・、ＰＯＳｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部２００８へ出力する。

【００９５】

（３）認証情報生成部２００８

認証情報生成部２００８において、実施の形態１の認証情報生成部１００８と異なる点についてのみ説明する。認証情報生成部１００８では、１つのヘッダ情報に対してのみ認証情報を作成していたが、認証情報生成部２００８においては、ｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）のそれぞれに対して、ｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）を作成する点が異なる。そして、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳ１、・・・、ＰＯＳｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部２００９へ出力する。

【００９６】

（４）暗号化部２００９

暗号化部２００９において、実施の形態１の暗号化部１００９と異なる点についてのみ説明する。暗号化部１００９では、１つのコンテンツ位置情報に対してのみ暗号化を行っていたが、暗号化部２００９においては、ｍ種類のコンテンツ位置情報（ＰＯＳ１、・・・、ＰＯＳｍ）のそれぞれに対して暗号化を行い、ｍ種類の暗号化コンテンツ位置情報（ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍ）を作成する点が異なる。そして、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の暗号化コンテンツ位置情報（ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化鍵束ＫＢと暗号化コンテンツＥＮＣＣＮＴを配布部２０１０へ出力する。

【００９７】

（５）配布部２０１０

配布部２０１０は、暗号化部２００９から入力されたｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の暗号化コンテンツ位置情報（ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化鍵束ＫＢと暗号化コ

ンテンツＥＮＣＣＮＴとを可搬媒体２１へ記録する。

【００９８】

＜配布センタ２０の動作＞

以上で、配布センタ２０の構成について説明を行ったが、ここでは配布センタ２０の動作の一例について、図１６に示すフローチャートの処理を行う。なお、配布センタ２０の動作に関しても、配布センタ１０同様、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【００９９】

ステップＳ１０１と同じ動作であるため、説明を省略する（ステップＳ２０１）。

ステップＳ１０２と同じ動作であるため、説明を省略する（ステップＳ２０２）。

コンテンツ位置情報生成部２００５は、暗号化鍵束生成部１００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）を生成する。そして、ｋ個の代表部分コンテンツをｍ種類選択し、各代表部分コンテンツに対応する特定情報を取得する。そして、ｋ個の代表部分コンテンツとｋ個の特定情報のｍ種類それぞれをヘッダ識別子と対応づけて、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとあわせて、ヘッダ情報生成部２００６へ出力する（ステップＳ２０３）。

【０１００】

ヘッダ情報生成部２００６は、コンテンツ位置情報生成部２００５から、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）と、ｋ組の代表部分コンテンツと特定情報をｍ種類と、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、特定情報の各々に対して、特定情報識別子を生成する。続いて、特定情報識別子と代表部分コンテンツと特定情報の各組に対して、代表部分コンテンツのハッシュ値を計算する。そして、その中から特定情報識別子と特定情報とだけを抽出し、特定情報識別子と特定情報とを含むコンテンツ位置情報をｍ種類と、特定情報識別子とハッシュ値とを含むヘッダ情報をｍ種類を、それぞれヘッダ識別子と対応づけて生成する。そして、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳ１、・・・、ＰＯＳｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部２００８へ出力する（ステップＳ２０４）。

【０１０１】

認証情報生成部２００８は、ヘッダ情報生成部２００６からｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳ１、・・・、ＰＯＳｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、認証情報生成情報格納部１００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ｍ種類のヘッダ情報ＨＥＡＤ１、・・・、ＨＥＡＤｍと認証情報生成情報ＧＥＮＡＵＴＨとを基に、ｍ種類の認証情報ＡＵＴＨ１、・・・、ＡＵＴＨｍをそれぞれ生成する。そして、ｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳＩＤ１、・・・、ＰＯＳＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部２００９へ出力する（ステップＳ２０５）。

【０１０２】

暗号化部２００９は、認証情報生成部２００８からｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・ＨＥＡＤＩＤｍ）とｍ種類のコンテンツ位置情報（ＰＯＳＩＤ１、・・・、ＰＯＳＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成し、同様にコンテンツ鍵ＣＫを基に、ｍ種

類のコンテンツ位置情報ＰＯＳ１、・・・、ＰＯＳｍを暗号化し、ｍ種類の暗号化コンテンツ位置情報ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍを生成する。そして、暗号化鍵束ＫＢとｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・ＨＥＡＤＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の暗号化コンテンツ位置情報（ＥＮＣＰＯＳＩＤ１、・・・、ＥＮＣＰＯＳＩＤｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化コンテンツＥＮＣＣＮＴとを配布部２０１０へ出力する（ステップＳ２０６）。

【０１０３】

配布部２０１０は、暗号化部２００９から入力された暗号化鍵束ＫＢとｍ種類のヘッダ識別子（ＨＥＡＤＩＤ１、・・・ＨＥＡＤＩＤｍ）とｍ種類のヘッダ情報（ＨＥＡＤ１、・・・、ＨＥＡＤｍ）とｍ種類の暗号化コンテンツ位置情報（ＥＮＣＰＯＳＩＤ１、・・・、ＥＮＣＰＯＳＩＤｍ）とｍ種類の認証情報（ＡＵＴＨ１、・・・、ＡＵＴＨｍ）と暗号化コンテンツＥＮＣＣＮＴとを可搬媒体２１へ記録する（ステップＳ２０７）。

【０１０４】

以上が、不正コンテンツ検知システム２の構成要素である配布センタ２０の構成と動作である。続いて、可搬媒体２１の構成について説明を行う。

＜可搬媒体２１の構成＞

可搬媒体２１は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のような可搬媒体であり、図１７に示すように、暗号化鍵束ＫＢとｍ種類のヘッダ識別子ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍとｍ種類のヘッダ情報ＨＥＡＤ１、・・・、ＨＥＡＤｍとｍ種類の暗号化コンテンツ位置情報ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍとｍ種類の認証情報ＡＵＴＨ１、・・・、ＡＵＴＨｍと暗号化コンテンツＥＮＣＣＮＴとが、配布センタ２０によって記録されているものである。

【０１０５】

以上が、不正コンテンツ検知システム２の構成要素である可搬媒体２１の構成である。続いて、実行装置２２の構成と動作について説明を行う。

＜実行装置２２の構成＞

実行装置２２は、図１８に示すように、取得部２２１、デバイス鍵格納部１２２、コンテンツ鍵取得部１２３、コンテンツ位置情報取得部１２４、検証情報格納部１２５、認証情報検証部１２６、部分復号化部１２７、ヘッダ情報検証部１２８、実行部１２９とから構成される。なお、デバイス鍵格納部１２２、コンテンツ鍵取得部１２３、コンテンツ位置情報取得部１２４、検証情報格納部１２５、認証情報検証部１２６、部分復号化部１２７、ヘッダ情報検証部１２８、実行部１２９については、実施の形態１の実行装置１２と同じ構成要素であるため、説明を省略する。

【０１０６】

（１）取得部２２１

取得部２２１は、まず、ｍ種類のヘッダ識別子ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍの中から一種類のヘッダ識別子を選択する。ｍ種類のヘッダ識別子ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍから一種類のヘッダ識別子を選択する方法は、乱数を用いてランダムに選択する方法や、前回選択したヘッダ識別子を記憶しておくことによってＨＥＡＤＩＤ１から順番に一つ一つ選択していく方法などがある。ここでは、ＨＥＡＤＩＤｉ（ＨＥＡＤＩＤｉはＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍのいずれか）を選択したとする。そして、可搬媒体２１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ識別子ＨＥＡＤＩＤｉに対応するヘッダ情報ＨＥＡＤｉ（ＨＥＡＤｉはＨＥＡＤ１、・・・、ＨＥＡＤｍのいずれか）と暗号化コンテンツ位置情報ＥＮＣＰＯＳｉ（ＥＮＣＰＯＳｉはＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｍのいずれか）と認証情報ＡＵＴＨｉ（ＡＵＴＨｉはＡＵＴＨ１、・・・、ＡＵＴＨｍのいずれか）と暗号化コンテンツＥＮＣＣＮＴを取得する。そして、その取得したヘッダ情報ＨＥＡＤｉと暗号化コンテンツ位置情報ＥＮＣＰＯＳｉと認証情報ＡＵＴＨｉをそれぞれ、ヘッダ情報ＨＥＡＤ、暗号化コンテンツ位置情報ＥＮＣＰＯＳ、認証情報ＡＵＴＨ、とする。そして、暗号化鍵束ＫＢとヘッダ

情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴをコンテンツ鍵取得部１２３へ出力する。

【０１０７】

＜実行装置２２の動作＞

以上で、実行装置２２の構成について説明を行ったが、ここで実行装置２２の動作について、図１９に示すフローチャートを用いて説明する。なお、実行装置２２の動作に関しても、実行装置１２同様、所望の結果が得られれば、各処理をどのような順番で行っても構わない。

【０１０８】

取得部２２１は、まず、ｍ種類のヘッダ識別子ＨＥＡＤＩＤ１、・・・、ＨＥＡＤＩＤｍから一種類のヘッダ識別子を選択する。ここでは、ＨＥＡＤＩＤｉ（ＨＥＡＤＩＤｉはＨＥＡＤ１、・・・、ＨＥＡＤｍのいずれか）を選択したとする。そして、可搬媒体２１に記録されているデータの読み取りを行った、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤｉと暗号化コンテンツ位置情報ＥＮＣＰＯＳｉと認証情報ＡＵＴＨｉと暗号化コンテンツＥＮＣＣＮＴを、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとして、コンテンツ鍵取得部１２３へ出力する。そして、コンテンツ鍵取得部１２３は、入力された暗号化鍵束ＫＢ、及び、デバイス鍵格納部１２２に格納されている鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと暗号化コンテンツ位置情報ＥＮＣＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴをコンテンツ位置情報取得部１２４へ出力する（ステップＳ２２１）。

【０１０９】

ステップＳ１２２と同じ動作であるので、説明を省略する（ステップＳ２２２）。
ステップＳ１２３と同じ動作であるので、説明を省略する（ステップＳ２２３）。
ステップＳ１２４と同じ動作であるので、説明を省略する（ステップＳ２２４）。
ステップＳ１２５と同じ動作であるので、説明を省略する（ステップＳ２２５）。
ステップＳ１２６と同じ動作であるので、説明を省略する（ステップＳ２２６）。

【０１１０】

ステップＳ１２７と同じ動作であるので、説明を省略する（ステップＳ２２７）。
ステップＳ１２８と同じ動作であるので、説明を省略する（ステップＳ２２８）。

以上が、不正コンテンツ検知システム２の構成要素である実行装置２２の構成と動作である。尚、コンテンツ鍵取得部１２３、コンテンツ位置情報取得部１２４、認証情報検証部１２６等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。

【０１１１】

ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

【０１１２】

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム２の効果＞

以上で、不正コンテンツ検知システム２について実施の形態に基づいて説明を行った。この不正コンテンツ検知システム２は、基本的に不正コンテンツ検知システム１と同様の効果を有するが、配布センタ２０が、一つのコンテンツＣＮＴに対し、複数の認証情報を

可搬媒体２１に記録するようにして、実行装置２２が、コンテンツＣＮＴの実行開始前に、複数の認証情報のいずれかの認証情報の正当性を検証し、それが正当な場合にのみ、コンテンツＣＮＴの実行を開始するようにした。つまり、複数の認証情報が可搬媒体２１に記録されているため、不正コンテンツ検知システム１に比べて、不正者による認証情報の偽造がより困難となり、安全性をより向上させることが出来るという効果を有する。

【０１１３】

（実施の形態３）

図２０は、本発明の実施の形態３における不正コンテンツ検知システムの構成図である。図２０において、配布センタ３０は外部からコンテンツＣＮＴを受け取り、後述する実行装置３２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体３１に記録するものであり、可搬媒体３１は実行装置３２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置３２は可搬媒体３１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。

【０１１４】

不正コンテンツ検知システム３は、配布センタ３０（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等の可搬媒体３１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、コンテンツＣＮＴを基に生成されるヘッダ情報ＨＥＡＤと、ヘッダ情報ＨＥＡＤの正当性を示す情報である認証情報ＡＵＴＨを、各実行装置３２へ配布する。各実行装置３２は、暗号化コンテンツＥＮＣＣＮＴを復号化してコンテンツＣＮＴを取得し、認証情報ＡＵＴＨが配布センタ３０によるヘッダ情報ＨＥＡＤの正規の認証情報であることと、ヘッダ情報ＨＥＡＤがコンテンツＣＮＴを基に生成されたものであることを確認し、コンテンツＣＮＴを実行開始する。

【０１１５】

以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム３の詳細について説明を行う。

＜不正コンテンツ検知システム３の構成＞

不正コンテンツ検知システム３は、図２０に示すように、配布センタ３０と、可搬媒体３１と、ｎ個の実行装置３２（ｎは１以上の自然数）から構成される。

【０１１６】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ３０の構成と動作について述べ、続いて可搬媒体３１の構成について述べ、最後に実行装置３２の構成と動作について述べる。

＜配布センタ３０の構成＞

配布センタ３０は、図２１に示すように、入力部３００１、コンテンツ鍵生成部３００２、実行装置情報格納部３００３、暗号化鍵束生成部３００４、コンテンツ位置情報生成部３００５、ヘッダ情報生成部３００６、認証情報生成情報格納部３００７、認証情報生成部３００８、暗号化部３００９、配布部３０１０から構成される。

【０１１７】

（１）入力部３００１

入力部３００１は、外部からコンテンツＣＮＴを入力出来るものである。入力部３００１は、例えば、可搬媒体であるＤＶＤ－ＲＯＭ等からコンテンツＣＮＴを読み取る機能を有する。外部から入力されるコンテンツＣＮＴは、実行装置３２で実行可能なフォーマット形式であって、例えば、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）２フォーマット形式による動画データやＭＰ３フォーマットによる音声データなどである。外部からコンテンツＣＮＴが入力された場合、そのコンテンツＣＮＴをコンテンツ鍵生成部３００２へ出力する。

【０１１８】

（２）コンテンツ鍵生成部３００２

コンテンツ鍵生成部３００２は、入力部３００１からコンテンツＣＮＴが入力された場

合、コンテンツ鍵ＣＫを生成する。コンテンツ鍵ＣＫを生成する方法としては、例えば、乱数を用いて１２８ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部３００２が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部３００４へ出力する。なお、コンテンツ鍵ＣＫはコンテンツＣＮＴを暗号化、復号化するための鍵であり、暗号化部３００９及び実行装置３２の部分復号化部３２７で使用される。

【０１１９】

（３）実行装置情報格納部３００３

実行装置情報格納部３００３は、複数の実行装置３２に与えられる鍵情報を保持するものである。図２２は、実行装置情報格納部３００３の一例を示しており、装置識別子ＡＩＤ１に対応付けられたデバイス鍵ＤＫ１と、装置識別子ＡＩＤ２に対応付けられたデバイス鍵ＤＫ２と、・・・、装置識別子ＡＩＤｎに対応付けられたデバイス鍵ＤＫｎを保持している状態を示している。ここで、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｎのそれぞれは、複数の実行装置３２のいずれかに対応付けられており、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｎのそれぞれは、対応する実行装置３２のデバイス鍵格納部３２２に格納されている鍵である。なお、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｎのそれぞれはコンテンツ鍵ＣＫを暗号化、復号化するための鍵であり、暗号化鍵束生成部３００４及びコンテンツ鍵取得部３２３で用いられる。例えば、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｎは、それぞれ異なる自然数１、２、・・・、ｎであり、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｎは、例えば、それぞれ異なる１２８ビット鍵データである。

【０１２０】

（４）暗号化鍵束生成部３００４

暗号化鍵束生成部３００４は、コンテンツ鍵生成部３００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴが入力された場合、実行装置情報格納部３００３にアクセスして複数の実行装置３２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢは、各実行装置３２がその暗号化鍵束ＫＢと自身の保持する鍵を用いてコンテンツ鍵ＣＫが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置３２はそれぞれ、ＡＩＤ１からＡＩＤｎのいずれかの装置識別子と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｎ）を保持しており、実行装置情報格納部３００３には、図２２のように、実行装置３２が保持する装置識別子（ＡＩＤ１、・・・、ＡＩＤｎ）と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｎ）の組が全て格納されているとする。そのような場合、暗号化鍵束ＫＢは例えば以下のように生成される。実行装置情報格納部３００３から装置識別子ＡＩＤ１と対応するデバイス鍵ＤＫ１を取得する。そして、デバイス鍵ＤＫ１を基にコンテンツ鍵ＣＫを暗号化し、暗号化コンテンツ鍵ＥＮＣＣＫ１＝Ｅｎｃ（ＤＫ１、ＣＫ）を生成し、装置識別子ＡＩＤ１に対応付ける。なお、Ｅｎｃ（Ｋ、Ｐ）を平文Ｐを暗号化鍵Ｋで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子（ＡＩＤ２、・・・、ＡＩＤｎ）とデバイス鍵（ＤＫ２、・・・、ＤＫｎ）に対しても同様の処理を行い、暗号化コンテンツ鍵ＥＮＣＣＫ２＝Ｅｎｃ（ＤＫ２、ＣＫ）、・・・、ＥＮＣＣＫｎ＝Ｅｎｃ（ＤＫｎ、ＣＫ）を生成し、装置識別子ＡＩＤ２、・・・、ＡＩＤｎに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のｎ組から構成される、図２３のような暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢをこのような構成にすることによって、各実行装置３２はその暗号化鍵束ＫＢと自身の保持するデバイス鍵（ＤＫ１、・・、ＤＫｎの何れか）を用いてコンテンツ鍵ＣＫが取得出来るようになる。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部３００５に出力する。なお、特許文献２などに記載の方法を用いることで、暗号化鍵束ＫＢの中の暗号化コンテンツ鍵（先程の例ではｎ個）の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵ＣＫを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部３００４で使用する暗号アルゴリズムは、例えば、非特許文献１に記載

のＡＥＳ方式（１２８ビット鍵）などであり、実行装置３２のコンテンツ鍵取得部３２３と同じ暗号アルゴリズムを用いる。

【０１２１】

（５）コンテンツ位置情報生成部３００５

コンテンツ位置情報生成部３００５は、暗号化鍵束生成部３００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、まずコンテンツＣＮＴを、図２４で示すようにｃ個（ｃは２以上の自然数）の部分コンテンツＣＮＴ－１、ＣＮＴ－２、ＣＮＴ－３、・・・、ＣＮＴ－ａ、・・・、ＣＮＴ－ｃに分割する。コンテンツＣＮＴをｃ個に分割する方法は、例えばコンテンツデータのある所定の区切り毎に分割する方法がある。ある所定の区切りの具体例としては、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、例えば、ＶＯＢ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ）ファイル単位や、ＶＯＢ単位や、ＶＯＢＵ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ　Ｕｎｉｔ）単位、セル（Ｃｅｌｌ）単位などである。コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、例えば、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、トラック単位、シリンダ単位などである。また、コンテンツデータの形式を問わず、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位などでも良い。なお、ＤＶＤ－Ｖｉｄｅｏ形式については、例えばインターネットアドレスhttp://positron.jfet.org/dvdvideo.htmlに記載されており、ＭＰＥＧ形式については、例えばインターネットアドレスhttp://www.pioneer.co.jp/crdl/tech/mpeg/1.htmlに記載されている。そして、ｃ個に分割された部分コンテンツのそれぞれを識別、特定出来る、ｃ個の特定情報ＡＤＤＲ１、・・・、ＡＤＤＲｃを取得する。このｃ個の特定情報の取得方法としては、例えば、所定の方法で区切った部分コンテンツに対して順番に番号（例えば１、２、・・、ｃ）を付けていく方法や、部分コンテンツの先頭を表すアドレス（物理アドレスや論理アドレスなど）と部分コンテンツのサイズを計算する方法や、コンテンツの先頭からの経過時間を計算する方法などがある。ここでは、部分コンテンツＣＮＴ－１を識別、特定する情報を特定情報ＡＤＤＲ１、部分コンテンツＣＮＴ－２を識別、特定する情報を特定情報ＡＤＤＲ２、部分コンテンツＣＮＴ－３を識別、特定する情報を特定情報ＡＤＤＲ３、・・・、部分コンテンツＣＮＴ－ａを特定する情報を特定情報ＡＤＤＲａ、・・・、部分コンテンツＣＮＴ－ｃを特定する情報を特定情報ＡＤＤＲｃとする。そして、部分コンテンツと特定情報のｃ組｛ＣＮＴ－１、ＡＤＤＲ１｝、｛ＣＮＴ－２、ＡＤＤＲ２｝、・・・、｛ＣＮＴ－ａ、ＡＤＤＲａ｝、・・・、｛ＣＮＴ－ｃ、ＡＤＤＲｃ｝を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫと併せて、ヘッダ情報生成部３００６へ出力する。

【０１２２】

なお、例えば、コンテンツＣＮＴが２時間の動画データで各部分コンテンツが１秒の動画データの場合、ｃは７２００となるが、ｃは２以上の自然数であればどのような値でも良い。さらに、それぞれの特定情報は、上記で紹介した情報に限らず、各部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。さらには、上記情報を複数組み合わせた情報であっても良い。

【０１２３】

（６）ヘッダ情報生成部３００６

ヘッダ情報生成部３００６は、コンテンツ位置情報生成部３００５から、部分コンテンツと特定情報のｃ組｛ＣＮＴ－１、ＡＤＤＲ１｝、｛ＣＮＴ－２、ＡＤＤＲ２｝、・・・、｛ＣＮＴ－ａ、ＡＤＤＲａ｝、・・・、｛ＣＮＴ－ｃ、ＡＤＤＲｃ｝と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤを生成する。まず、ｃ組の部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。特定情報識別子を生成する方法としては、自然数を順番に割り当てていく（１、２、・・・、ｃ）方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した特定情報識別子をそれぞれ、ＡＤＤＲＩＤ１、ＡＤＤＲＩＤ２、・・・ＡＤＤＲＩＤａ、・・・、ＡＤＤＲＩＤｃとし、次のように特定情報

識別子と部分コンテンツと特定情報とが対応しているとする。｛ＡＤＤＲＩＤ１、ＣＮＴ―１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ２、ＣＮＴ―２、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤａ、ＣＮＴ―ａ、ＡＤＤＲａ｝、・・・、｛ＡＤＤＲＩＤｃ、ＣＮＴ―ｃ、ＡＤＤＲｃ｝。続いて、ｃ組の特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値としてハッシュ値を計算する。部分コンテンツのハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置３２のヘッダ情報検証部３２８で用いる方法と同じものを用いる。ここで、各組に対して計算したハッシュ値をそれぞれ、ＨＡＳＨ１、ＨＡＳＨ２、・・・、ＨＡＳＨａ、・・・、ＨＡＳＨｃとし、次のように特定情報識別子と部分コンテンツと特定情報とハッシュ値が対応しているとする。｛ＡＤＤＲＩＤ１、ＣＮＴ―１、ＡＤＤＲ１、ＨＡＳＨ１｝、｛ＡＤＤＲＩＤ２、ＣＮＴ―２、ＡＤＤＲ２、ＨＡＳＨ２｝、・・・、｛ＡＤＤＲＩＤａ、ＣＮＴ―ａ、ＡＤＤＲａ、ＨＡＳＨａ｝、・・・、｛ＡＤＤＲＩＤｃ、ＣＮＴ―ｃ、ＡＤＤＲｃ、ＨＡＳＨｃ｝。そして、その中から特定情報識別子と特定情報だけを抽出し、図２５で示すような、特定情報識別子と特定情報とからなるコンテンツ位置情報ＰＯＳ＝｛ＡＤＤＲＩＤ１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ２、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤａ、ＡＤＤＲａ｝、・・・、｛ＡＤＤＲＩＤｃ、ＡＤＤＲｃ｝を生成する。また、特定情報識別子とハッシュ値だけを抽出し、図２６で示すような、特定情報識別子とハッシュ値とからなるヘッダ情報ＨＥＡＤ＝｛ＡＤＤＲＩＤ１、ＨＡＳＨ１｝、｛ＡＤＤＲＩＤ２、ＨＡＳＨ２｝、・・・、｛ＡＤＤＲＩＤａ、ＨＡＳＨａ｝、・・・、｛ＡＤＤＲＩＤｃ、ＨＡＳＨｃ｝を生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部３００８へ出力する。

【０１２４】

（７）認証情報生成情報格納部３００７

認証情報生成情報格納部３００７は、ヘッダ情報ＨＥＡＤの認証情報である認証情報ＡＵＴＨを生成するための、認証情報生成情報ＧＥＮＡＵＴＨを保持するものである。この認証情報生成情報ＧＥＮＡＵＴＨは、例えば、デジタル署名アルゴリズムの署名生成鍵（秘密鍵）である。認証情報生成情報ＧＥＮＡＵＴＨに対応する検証情報ＶＥＲは、実行装置３２の検証情報格納部３２５に格納されている。この検証情報ＶＥＲは、例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。

【０１２５】

（８）認証情報生成部３００８

認証情報生成部３００８は、ヘッダ情報生成部３００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤに含まれるｃ個のハッシュ値を連結した値に対する認証情報である認証情報ＡＵＴＨを生成する。まず、認証情報生成情報格納部３００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤに含まれるｃ個のハッシュ値と認証情報生成情報ＧＥＮＡＵＴＨを用いて、ヘッダ情報ＨＥＡＤに含まれるｃ個のハッシュ値を連結した値に対する認証情報である認証情報ＡＵＴＨを生成する。なお、認証情報ＡＵＴＨの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズム（非特許文献１に記載のＤＳＡ方式）を用いる方法の一例を、図２７を用いて説明する。まず、ヘッダ情報ＨＥＡＤのｃ個全てのハッシュ値を結合した値ＨＡＳＨ１｜｜ＨＡＳＨ２｜｜・・・｜｜ＨＡＳＨａ｜｜・・｜｜ＨＡＳＨｃに対する属性値（例：ハッシュ値）として、結合ハッシュ値＝ＯＷＦ（ＨＡＳＨ１｜｜ＨＡＳＨ２｜｜・・・｜｜ＨＡＳＨａ｜｜・・｜｜ＨＡＳＨｃ）を生成する。そして、その結合ハッシュ値に対するデジタル署名を作成する。ここで、ＧＥＮＳＩＧ（Ｋ、Ｍ）を署名生成鍵Ｋを用いてメッセージＭに対して生成されたデジタル署名とすると、認証情報ＡＵＴＨは、ＡＵＴＨ＝ＧＥＮＳＩＧ（ＧＥＮＡＵ

ＴＨ、ＯＷＦ（ＨＡＳＨ１｜｜ＨＡＳＨ２｜｜・・・｜｜ＨＡＳＨｃ））となる。ここで、ＯＷＦ（Ｘ）は、一方向性関数（例えば、ＳＨＡ－１アルゴリズム）にＸを入力した際の出力値とする。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部３００９へ出力する。なお、認証情報生成部３００８で使用するデジタル署名アルゴリズムは、実行装置３２の認証情報検証部３２５で用いるデジタル署名アルゴリズムと同じものを用いる。

【０１２６】

（９）暗号化部３００９

暗号化部３００９は、認証情報生成部３００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして暗号化コンテンツＥＮＣＣＮＴを生成する。コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。この暗号化コンテンツＥＮＣＣＮＴの生成方法としては、例えば、以下のような方法がある。まず、コンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ－１を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ－１＝Ｅｎｃ（ＣＫ、ＣＮＴ－１）を生成する。続いて、同じコンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ－２を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ－２＝Ｅｎｃ（ＣＫ、ＣＮＴ－２）を生成する。これを繰り返して、図２８で示すようなｃ個の暗号化部分コンテンツＥＮＣＣＮＴ－１、・・・、ＥＮＣＣＮＴ－ａ、・・・、ＥＮＣＣＮＴ－ｃから構成される暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを配布部３０１０へ出力する。暗号化部３００９で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置３２の部分復号化部３２７と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツＥＮＣＣＮＴの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵ＣＫで暗号化していたが、非特許文献１に記載のブロック暗号のモードを利用してもよい。例えば、ＣＢＣモードやＯＦＢモード、ＣＦＢモードなどでもよく、さらに、ある一定間隔毎にモード（例：ＣＢＣモード）の初期値を変化させるようにしたものでも良い。さらに、暗号化を行う単位は、コンテンツ位置情報生成部３００５でコンテンツＣＮＴを分割した単位に限るものではなく、例えば１６バイト毎であっても良い。

【０１２７】

（１０）配布部３０１０

配布部３０１０は、暗号化部３００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを可搬媒体３１へ記録するものである。例えば、可搬媒体３１が書き込み可能な光ディスクであり、配布部３０１０は書き込み用レーザー等を用いてデータを記録する。

【０１２８】

＜配布センタ３０の動作＞

以上で、配布センタ３０の構成について説明を行ったが、ここでは配布センタ３０の動作の一例について、図２９に示すフローチャートの処理を行う。なお、配布センタ３０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【０１２９】

入力部３００１は、外部から入力されたコンテンツＣＮＴをコンテンツ鍵生成部３００２へ出力し、コンテンツ鍵生成部３００２は、コンテンツ鍵ＣＫを生成し、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部３００４へ出力する（ステップＳ３０１）。

暗号化鍵束生成部３００４は、コンテンツ鍵生成部３００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴを入力され、実行装置情報格納部３００３にアクセスして複数の実行装

置３２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部３００５に出力する（ステップＳ３０２）。

【０１３０】

コンテンツ位置情報生成部３００５、暗号化鍵束生成部３００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫを入力され、コンテンツＣＮＴをｃ個の部分コンテンツに分割し、そのｃ個の部分コンテンツのそれぞれを識別、特定するｃ個の特定情報を取得する。そして、ｃ組の部分コンテンツと特定情報を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとあわせて、ヘッダ情報生成部３００６へ出力する（ステップＳ３０３）。

【０１３１】

ヘッダ情報生成部３００６は、コンテンツ位置情報生成部３００５から、ｃ組の部分コンテンツと特定情報と、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、ｃ組の部分コンテンツと特定情報の各組に対して、特定情報識別子を生成する。続いて、ｃ組の特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値としてハッシュ値を計算する。そして、特定情報識別子と特定情報を抽出し、ｃ組の特定情報識別子と特定情報とからなるコンテンツ位置情報ＰＯＳを生成する。さらに、ｃ組の特定情報識別子とハッシュ値とからなるヘッダ情報ＨＥＡＤを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部３００８へ出力する（ステップＳ３０４）。

【０１３２】

認証情報生成部３００８は、ヘッダ情報生成部３００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、認証情報生成情報格納部３００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤと認証情報生成情報ＧＥＮＡＵＴＨとを用いて、ヘッダ情報ＨＥＡＤに対する認証情報である認証情報ＡＵＴＨを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部３００９へ出力する（ステップＳ３０５）。

【０１３３】

暗号化部３００９は、認証情報生成部３００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを配布部３０１０へ出力する（ステップＳ３０６）。

【０１３４】

配布部３０１０は、暗号化部３００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを可搬媒体３１へ記録する（ステップＳ３０７）。

以上が、不正コンテンツ検知システム３の構成要素である配布センタ３０の構成と動作である。続いて、可搬媒体３１の構成について説明を行う。

【０１３５】

＜可搬媒体３１の構成＞

可搬媒体３１は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のような光ディスクの媒体（メディア）であり、図３０に示すように、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが配布センタ３０によって記録されているものとする。

【０１３６】

以上が、不正コンテンツ検知システム３の構成要素である可搬媒体３１の構成である。続いて、実行装置３２の構成と動作について説明を行う。

＜実行装置３２の構成＞

実行装置３２は、図３１に示すように、取得部３２１、デバイス鍵格納部３２２、コンテンツ鍵取得部３２３、検証情報格納部３２４、認証情報検証部３２５、特定情報選択部３２６、部分復号化部３２７、ヘッダ情報検証部３２８、実行部３２９とから構成される。

【０１３７】

（１）取得部３２１

取得部３２１は、可搬媒体３１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを取得する。そして、取得した暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ鍵取得部３２３へ出力する。

【０１３８】

（２）デバイス鍵格納部３２２

デバイス鍵格納部３２２は、配布センタ３０の実行装置情報格納部３００３の中の鍵情報の一部を保持するものであり、デバイス鍵格納部３２２に与えられる鍵情報と暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫが取得出来るものである。例えば、実行装置情報格納部３００３が図２２のような場合、デバイス鍵格納部３２２には、装置識別子ＡＩＤｉとデバイス鍵Ｋｉ（ｉは１からｎのいずれか）が与えられる。

【０１３９】

（３）コンテンツ鍵取得部３２３

コンテンツ鍵取得部３２３は、取得部３２１から暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、デバイス鍵格納部３２２に格納されている鍵情報及び暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫを取得する。例えば、暗号化鍵束ＫＢが図２３のような場合で、デバイス鍵格納部３２２には装置識別子ＡＩＤｉとデバイス鍵ＤＫｉ（ｉは１からｎのいずれか）が与えられている場合、コンテンツ鍵取得部３２３はデバイス鍵格納部３２２から装置識別子ＡＩＤｉとデバイス鍵ＤＫｉを取得し、暗号化鍵束ＫＢの中から装置識別子ＡＩＤｉに対応する暗号化コンテンツ鍵ＥＮＣＣＫｉ（ＥＮＣＣＫ１からＥＮＣＣＫｎの何れか）を取得する。そしてデバイス鍵ＤＫｉを基に、暗号化コンテンツ鍵ＥＮＣＣＫｉを復号化することによって、コンテンツ鍵ＣＫ＝Ｄｅｃ（ＤＫｉ、ＥＮＣＣＫｉ）を取得する。なお、Ｄｅｃ（Ｋ、Ｃ）を暗号文Ｃを復号化鍵Ｋを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを認証情報検証部３２５へ出力する。

【０１４０】

（４）検証情報格納部３２４

検証情報格納部３２４は、ヘッダ情報ＨＥＡＤに対する認証情報である認証情報ＡＵＴＨの正当性を検証するために必要な検証情報ＶＥＲを保持するものである。この検証情報ＶＥＲに対応する認証情報生成情報ＧＥＮＡＵＴＨは、配布センタ３０の認証情報生成情報格納部３００７に格納されている。例えば、検証情報ＶＥＲはデジタル署名アルゴリズムの署名検証鍵（公開鍵）である。

【０１４１】

（５）認証情報検証部３２５

認証情報検証部３２５は、コンテンツ鍵取得部３２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、検証情報格納部３２５に格納されている検証情報ＶＥＲを使って、認証情報ＡＵＴＨが発行センタ３０によるヘッダ情報ＨＥＡＤの正規の認証情報であ

るかを検証する。例えば、デジタル署名検証アルゴリズムを用いて、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤの正しいデジタル署名であるかを検証するなどである。このデジタル署名検証アルゴリズムは、配布センタ３０の認証情報生成部３００８で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。ここでは、図３２を用いて、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤの正しい認証情報であるかを検証する方法の一例を説明する。まず、ヘッダ情報ＨＥＡＤのｃ個全てのハッシュ値を結合した値ＨＡＳＨ１｜｜ＨＡＳＨ２｜｜・・・｜｜ＨＡＳＨａ｜｜・・｜｜ＨＡＳＨｃに対する属性値（例：ハッシュ値）として、結合ハッシュ値＝ＯＷＦ（ＨＡＳＨ１｜｜ＨＡＳＨ２｜｜・・・｜｜ＨＡＳＨａ｜｜・・｜｜ＨＡＳＨｃ）を生成する。そして、認証情報ＡＵＴＨがその結合ハッシュ値に対する正規のデジタル署名であるか検証する。なお、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。認証情報検証部３２５は、認証情報ＡＵＴＨが発行センタ３０によるヘッダ情報ＨＥＡＤの正しい認証情報である場合にのみ、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴを特定情報選択部３２６へ出力する。

【０１４２】

（６）特定情報選択部３２６

特定情報選択部３２６は、認証情報検証部３２５からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、ヘッダ情報ＨＥＡＤに含むｃ個の特定情報識別子（ＰＯＳＩＤ１、・・・、ＰＯＳＩＤｃ）の中から、ｂ個の特定情報識別子（ｂは１以上ｃ－１以下の自然数）を選択する。ここでは、第三者によってどの特定情報識別子が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、特定情報選択部３２６が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献２が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、特定情報選択部３２６が温度センサや湿度センサを有することにより実現出来る。その後、選択されたｂ個の特定情報識別子と対応するｂ個のハッシュ値から成る被選択ヘッダ情報ＳＥＬＨＥＡＤを生成する。例として、図３３は、特定情報識別子ＡＤＤＲＩＤ２とハッシュ値ＨＡＳＨ２、特定情報識別子ＡＤＤＲＩＤａとハッシュ値ＨＡＳＨａを選択した場合の被選択ヘッダ情報ＳＥＬＨＥＡＤについて表している。また、選択されたｂ個の特定情報識別子と対応するｂ個の特定情報から成る被選択コンテンツ位置情報ＳＥＬＰＯＳを生成する。例として、図３４は、特定情報識別子ＡＤＤＲＩＤ２と特定情報ＡＤＤＲ２、特定情報識別子ＡＤＤＲＩＤａと特定情報ＡＤＤＲａを選択した場合の被選択コンテンツ位置情報ＳＥＬＰＯＳについて表している。そして、コンテンツ鍵ＣＫと被選択ヘッダ情報ＳＥＬＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと暗号化コンテンツＥＮＣＣＮＴとを部分復号化部３２７へ出力する。ここで、被選択ヘッダ情報ＳＥＬＨＥＡＤにはｂ組の特定情報識別子とハッシュ値を、被選択コンテンツ位置情報ＳＥＬＰＯＳにはｂ組の特定情報識別子と特定情報を含むことになる。なお、パラメータｂは、システムパラメータ（全ての実行装置３２に予め共有に与えられているパラメータ）であってもよいし、各実行装置３２に個別に予め与えられているパラメータであってもよい。

【０１４３】

（７）部分復号化部３２７

部分復号化部３２７は、特定情報選択部３２６からコンテンツ鍵ＣＫと被選択ヘッダ情報ＳＥＬＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、以下の処理を行う。まず、被選択コンテンツ位置情報ＳＥＬＰＯＳの中の一組目の特定情報識別子と特定情報を抽出する。ここでは被選択コンテンツ位置情報ＳＥＬＰＯＳが図３４の場合を例に挙げ、一組目の特定情報識別子と特定情報をそれぞれＡＤＤＲＩＤ２とＡＤＤＲ２とする。そして、暗号化コンテンツＥＮＣＣＮＴの中

から特定情報ＡＤＤＲ２が特定する暗号化部分コンテンツＥＮＣＣＮＴ－２を取得し、コンテンツ鍵ＣＫを基に復号化を行い、部分コンテンツＣＮＴ－２を取得する（例えば、図３５参照）。続いて、被選択コンテンツ位置情報ＳＥＬＰＯＳの二組目以降の特定情報識別子と特定情報とを同様に抽出し、対応する部分コンテンツを取得する。そして、被選択ヘッダ情報ＳＥＬＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、抽出されたｂ組の特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、をヘッダ情報検証部３２８へ出力する。なお、部分復号化部３２７で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式などであり、配布センタ３０の暗号化部３００９と同じ暗号アルゴリズムを用いる。

【０１４４】

（８）ヘッダ情報検証部３２８

ヘッダ情報検証部３２８は、部分復号化部３２７から被選択ヘッダ情報ＳＥＬＨＥＡＤとコンテンツＣＮＴと、ｂ組の特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、が入力された場合、まず、一組目の特定情報識別子と部分コンテンツに対して、以下の処理を行う。ここでも被選択コンテンツ位置情報ＳＥＬＰＯＳが図３４の場合を例に挙げて、一組目の特定情報識別子と部分コンテンツをそれぞれＡＤＤＲＩＤ２とＣＮＴ－２とする。最初に、部分コンテンツＣＮＴ－２に対して、そのハッシュ値Ｘを計算する。部分コンテンツのハッシュ値を求める方法としては、例えば、一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、配布センタ３０のヘッダ情報生成部３００８で用いる方法と同じものを用いる。そして、被選択ヘッダ情報ＳＥＬＨＥＡＤの中の特定情報識別子ＡＤＤＲＩＤ２に対応するハッシュ値ＨＡＳＨ２と計算されたハッシュ値Ｘが等しいかどうか確認する。もし、同じ値であれば、二組目以降の特定情報識別子と部分コンテンツに対しても、同様にしてハッシュ値を計算し、被選択ヘッダ情報ＳＥＬＨＥＡＤの中の対応する特定情報識別子のハッシュ値と比較する。ここで、ｂ個のハッシュ値が全て等しかった場合にのみ、ヘッダ情報検証部３２８は実行部３２９へ暗号化コンテンツＥＮＣＣＮＴとコンテンツ鍵ＣＫと、を出力する。

【０１４５】

（９）実行部３２９

実行部３２９は、ヘッダ情報検証部３２８から入力された暗号化コンテンツＥＮＣＣＮＴに含まれるｃ個の暗号化部分コンテンツＥＮＣＣＮＴ－１、・・・、ＥＮＣＣＮＴ－ｃを、コンテンツ鍵ＣＫを基に逐次復号化を行って部分コンテンツＣＮＴ－１、・・・、ＣＮＴ－ｃを取得し、逐次その部分コンテンツを実行するものである。例えば、実行部３２９はＭＰＥＧ２データやＭＰ３データをデコードする機能を有するデコータを有していて、ＭＰＥＧ２形式の動画コンテンツやＭＰ３形式の音声コンテンツであるコンテンツＣＮＴを逐次デコードして、外部に出力するようにしても良い。また例えば、実行部３２９は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生しても良いし、別の可搬媒体や記録媒体にコンテンツデータを出力しても良いし、コンテンツデータを紙などに印刷してもよい。なお、復号化を行う単位やデコードを行う単位は、コンテンツ位置情報生成部３００５でコンテンツＣＮＴを分割した単位に限るものではなく、例えば１６バイト毎であっても良い。

【０１４６】

＜実行装置３２の動作＞

以上で、実行装置３２の構成について説明を行ったが、ここで実行装置３２の動作について、図３６に示すフローチャートを用いて説明する。なお、実行装置３２の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【０１４７】

取得部３２１は、可搬媒体３１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コン

テンツＥＮＣＣＮＴとをコンテンツ鍵取得部３２３へ出力する。そして、コンテンツ鍵取得部３２３は、入力された暗号化鍵束ＫＢ及びデバイス鍵格納部３２２が保持している鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを認証情報検証部３２５へ出力する（ステップＳ３２１）。

【０１４８】

認証情報検証部３２５は、コンテンツ鍵取得部３２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを入力された場合、検証情報格納部３２４に格納されている検証情報ＶＥＲを用いて、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する正しい認証情報であるかを検証する（ステップＳ３２２）。

【０１４９】

認証情報検証部３２５は、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する発行センタ３０の正しい認証情報である場合にのみ、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとを特定情報選択部３２６へ出力し、ステップＳ３２４へ進む。もし、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する正しい認証情報ではない場合、処理を終了する（ステップＳ３２３）。

【０１５０】

特定情報選択部３２６は、認証情報検証部３２５からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとを入力された場合、コンテンツ位置情報ＰＯＳに含まれるｃ個の特定情報識別子からｂ個の特定情報識別子を選択する。そして、ヘッダ情報ＨＥＡＤから選択されたｂ個の特定情報識別子と対応するｂ個のハッシュ値からなる被選択ヘッダ情報ＳＥＬＨＥＡＤを生成する。また、コンテンツ位置情報ＰＯＳから選択されたｂ個の特定情報識別子と対応するｂ個の特定情報からなる被選択コンテンツ位置情報ＳＥＬＰＯＳを生成する。そして、コンテンツ鍵ＣＫと被選択ヘッダ情報ＳＥＬＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを部分復号化部３２７へ出力する（ステップＳ３２４）。

【０１５１】

部分復号化部３２７は、特定情報選択部３２６からコンテンツ鍵ＣＫと被選択ヘッダ情報ＳＥＬＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと暗号化コンテンツＥＮＣＣＮＴとを入力される。そして、コンテンツ鍵ＣＫを基に、暗号化コンテンツＥＮＣＣＮＴに含まれるｂ個の特定情報のそれぞれに対する暗号化部分コンテンツをそれぞれ復号化し、ｂ個の部分コンテンツを抽出する。そして、被選択ヘッダ情報ＳＥＬＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、ｂ組の特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、をヘッダ情報検証部３２８へ出力する（ステップＳ３２５）。

【０１５２】

ヘッダ情報検証部３２８は、部分復号化部３２７から被選択ヘッダ情報ＳＥＬＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴと、ｂ組の特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、を入力される。そして、各組の部分コンテンツに対して、そのハッシュ値を計算する（ステップＳ３２６）。

ヘッダ情報検証部３２８は、計算したハッシュ値が、被選択ヘッダ情報ＳＥＬＨＥＡＤの中の特定情報識別子に対応するハッシュ値と等しいかどうか確認し、もし、全てのハッシュ値が同じ値であれば、ヘッダ情報検証部３２８は実行部３２９へ暗号化コンテンツＥＮＣＣＮＴとコンテンツ鍵ＣＫを出力し、ステップＳ３２８へ進む。もし、一つでもハッシュ値が一致しなければ、処理を終了する（ステップＳ３２７）。

【０１５３】

実行部３２９は、ヘッダ情報検証部３２８から受け取った暗号化コンテンツＥＮＣＣＮＴの中の暗号化部分コンテンツを、コンテンツ鍵を用いて逐次復号化し、その部分コンテンツを実行する（ステップＳ３２８）。

以上が、不正コンテンツ検知システム３の構成要素である実行装置３２の構成と動作である。尚、コンテンツ鍵取得部３２３、認証情報検証部３２５、特定情報選択部３２６等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。

【０１５４】

ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

【０１５５】

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム３の効果＞

以上、不正コンテンツ検知システム３について実施の形態に基づいて説明したが、この不正コンテンツ検知システム３においては、配布センタ３０が、暗号化されたコンテンツＣＮＴとともに、コンテンツＣＮＴに対応するヘッダ情報ＨＥＡＤ、及び、ヘッダ情報に対する認証情報ＡＵＴＨ（例えばデジタル署名）、及び、コンテンツ位置情報ＰＯＳを可搬媒体３１に記録するようにした。そして、実行装置３２が、コンテンツＣＮＴの実行、再生開始前に、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに対する正規の認証情報（例えばデジタル署名）であるか検証するとともに、ヘッダ情報ＨＥＡＤに含まれるｃ個のハッシュ値のうち、ｂ個のハッシュ値に絞って検証するようにした。これは、コンテンツＣＮＴを実行、再生開始する毎に、異なるハッシュ値を選択するようにして、不正者は、どのハッシュ値が選択されるか予想出来ないように注意する。そして、選択されたｂ個のハッシュ値が共に正当であると検証された場合にのみ、コンテンツＣＮＴの実行、再生を開始するようにした。そうすることにより、実行装置３２は、不正な認証情報ＡＵＴＨもしくはヘッダ情報ＨＥＡＤもしくはコンテンツＣＮＴが記録された可搬媒体３１のコンテンツＣＮＴは実行開始しないようになる。これにより、コンテンツＣＮＴの中のある部分コンテンツを不正な部分コンテンツに差し替えようとしても、その不正な部分コンテンツに差し替えられた部分に対応するハッシュ値の検証が行われた場合、そのコンテンツは実行出来なくなる。つまり、コンテンツＣＮＴの一部分でも不正な部分コンテンツに差し替えた場合、ある確率でコンテンツＣＮＴを実行できなくなることになる。これは、コンテンツＣＮＴの中の一部分を、不正なコンテンツに差し替えられるような攻撃を防ぐ抑止力となる。

【０１５６】

また、実行装置３２は、認証情報ＡＵＴＨの正当性の検証を、コンテンツＣＮＴを実行、再生開始する前に全て行うため、コンテンツＣＮＴの実行、再生中の特別な処理が必要なくなり、コンテンツＣＮＴの実行中の処理負荷が軽減されるという効果を有する。

（実施の形態４）

図３７は、本発明の実施の形態４における不正コンテンツ検知システムの構成図である。図３７において、配布センタ４０は外部からコンテンツＣＮＴを受け取り、後述する実行装置４２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体４１に記録するものであり、可搬媒体４１は実行装置４２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置４２は可搬媒体４１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。

【０１５７】

不正コンテンツ検知システム４は、配布センタ４０（正規のコンテンツ提供者、著作権

者、正規の光ディスクプレス業者など）が、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等の可搬媒体４１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、コンテンツＣＮＴを基に生成されるヘッダ情報ＨＥＡＤと、ヘッダ情報ＨＥＡＤの正当性を示す情報である認証情報ＡＵＴＨを、各実行装置４２へ配布する。各実行装置４２は、暗号化コンテンツＥＮＣＣＮＴを復号化してコンテンツＣＮＴを取得し、コンテンツＣＮＴを基にヘッダ情報ＨＥＡＤを再生成し、認証情報ＡＵＴＨが配布センタ４０によるヘッダ情報ＨＥＡＤの正規の認証情報であることを確認し、コンテンツＣＮＴを実行開始する。

【０１５８】

以上が、本実施形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施形態である不正コンテンツ検知システム４の詳細について説明を行う。

＜不正コンテンツ検知システム４の構成＞

不正コンテンツ検知システム４は、図３７に示すように、配布センタ４０と、可搬媒体４１と、ｎ個の実行装置４２（ｎは１以上の自然数）から構成される。

【０１５９】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ４０の構成と動作について述べ、続いて可搬媒体４１の構成について述べ、最後に実行装置４２の構成と動作について述べる。

＜配布センタ４０の構成＞

配布センタ４０は、図３８に示すように、入力部４００１、コンテンツ鍵生成部４００２、実行装置情報格納部４００３、暗号化鍵束生成部４００４、コンテンツ位置情報生成部４００５、ヘッダ情報生成部４００６、認証情報生成情報格納部４００７、認証情報生成部４００８、暗号化部４００９、配布部４０１０から構成される。

【０１６０】

（１）入力部４００１

入力部４００１は、外部からコンテンツＣＮＴを入力出来るものである。入力部４００１は、例えば、可搬媒体であるＤＶＤ－ＲＯＭ等からコンテンツＣＮＴを読み取る機能を有する。外部から入力されるコンテンツＣＮＴは、実行装置４２で実行可能なフォーマット形式であって、例えば、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）２フォーマット形式による動画データやＭＰ３フォーマットによる音声データなどである。外部からコンテンツＣＮＴが入力された場合、そのコンテンツＣＮＴをコンテンツ鍵生成部４００２へ出力する。

【０１６１】

（２）コンテンツ鍵生成部４００２

コンテンツ鍵生成部４００２は、入力部４００１からコンテンツＣＮＴが入力された場合、コンテンツ鍵ＣＫを生成する。コンテンツ鍵ＣＫを生成する方法としては、例えば、乱数を用いて１２８ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部４００２が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部４００４へ出力する。なお、コンテンツ鍵ＣＫはコンテンツＣＮＴを暗号化、復号化するための鍵であり、暗号化部４００９及び実行装置４２の部分復号化部４２７で使用される。

【０１６２】

（３）実行装置情報格納部４００３

実行装置情報格納部４００３は、複数の実行装置４２に与えられる鍵情報を保持するものである。図３９は、実行装置情報格納部４００３の一例を示しており、装置識別子ＡＩＤ１に対応付けられたデバイス鍵ＤＫ１と、装置識別子ＡＩＤ２に対応付けられたデバイス鍵ＤＫ２と、・・・、装置識別子ＡＩＤｎに対応付けられたデバイス鍵ＤＫｎを保持している状態を示している。ここで、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｎのそれぞれは、複数の実行装置４２のいずれかに対応付けられており、デバイス鍵ＤＫ１、

ＤＫ２、・・・、ＤＫｎのそれぞれは、対応する実行装置４２のデバイス鍵格納部４２２に格納されている鍵である。なお、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｎのそれぞれはコンテンツ鍵ＣＫを暗号化、復号化するための鍵であり、暗号化鍵束生成部４００４及びコンテンツ鍵取得部４２３で用いられる。例えば、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｎは、それぞれ異なる自然数１、２、・・・、ｎであり、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｎは、例えば、それぞれ異なる１２８ビット鍵データである。

【０１６３】

（４）暗号化鍵束生成部４００４

暗号化鍵束生成部４００４は、コンテンツ鍵生成部４００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴが入力された場合、実行装置情報格納部４００３にアクセスして複数の実行装置４２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢは、各実行装置４２がその暗号化鍵束ＫＢと自身の保持する鍵を用いてコンテンツ鍵ＣＫが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置４２はそれぞれ、ＡＩＤ１からＡＩＤｎのいずれかの装置識別子と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｎ）を保持しており、実行装置情報格納部４００３には、図３９のように、実行装置４２が保持する装置識別子（ＡＩＤ１、・・・、ＡＩＤｎ）と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｎ）の組が全て格納されているとする。そのような場合、暗号化鍵束ＫＢは例えば以下のように生成される。実行装置情報格納部４００３から装置識別子ＡＩＤ１と対応するデバイス鍵ＤＫ１を取得する。そして、デバイス鍵ＤＫ１を基にコンテンツ鍵ＣＫを暗号化し、暗号化コンテンツ鍵ＥＮＣＣＫ１＝Ｅｎｃ（ＤＫ１、ＣＫ）を生成し、装置識別子ＡＩＤ１に対応付ける。なお、Ｅｎｃ（Ｋ、Ｐ）を平文Ｐを暗号化鍵Ｋで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子（ＡＩＤ２、・・・、ＡＩＤｎ）とデバイス鍵（ＤＫ２、・・・、ＤＫｎ）に対しても同様の処理を行い、暗号化コンテンツ鍵ＥＮＣＣＫ２＝Ｅｎｃ（ＤＫ２、ＣＫ）、・・・、ＥＮＣＣＫｎ＝Ｅｎｃ（ＤＫｎ、ＣＫ）を生成し、装置識別子ＡＩＤ２、・・・、ＡＩＤｎに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のｎ組から構成される、図４０のような暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢをこのような構成にすることによって、各実行装置４２はその暗号化鍵束ＫＢと自身の保持するデバイス鍵（ＤＫ１、・・、ＤＫｎの何れか）を用いてコンテンツ鍵ＣＫが取得出来るようになる。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部４００５に出力する。なお、特許文献２などに記載の方法を用いることで、暗号化鍵束ＫＢの中の暗号化コンテンツ鍵（先程の例ではｎ個）の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵ＣＫを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部４００４で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置４２のコンテンツ鍵取得部４２３と同じ暗号アルゴリズムを用いる。

【０１６４】

（５）コンテンツ位置情報生成部４００５

コンテンツ位置情報生成部４００５は、暗号化鍵束生成部４００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、まずコンテンツＣＮＴを、図４１で示すようにｃ個（ｃは２以上の自然数）の部分コンテンツＣＮＴ－１、ＣＮＴ－２、ＣＮＴ－３、・・・、ＣＮＴ－ａ、・・・、ＣＮＴ－ｃに分割する。コンテンツＣＮＴをｃ個に分割する方法は、例えばコンテンツデータのある所定の区切り毎に分割する方法がある。ある所定の区切り方の具体例としては、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、例えば、ＶＯＢ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ）ファイル単位や、ＶＯＢ単位や、ＶＯＢＵ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ　Ｕｎｉｔ）単位、セル（Ｃｅｌｌ）単位などである。コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、例えば、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、トラック単

位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（ＥＣＣブロック単位）などである。また、コンテンツデータの形式を問わず、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位などでも良い。なお、ＤＶＤ－Ｖｉｄｅｏ形式については、例えばインターネットアドレスhttp://positron.jfet.org/dvdvideo.htmlに記載されており、ＭＰＥＧ形式については、例えばインターネットアドレスhttp://www.pioneer.co.jp/crdl/tech/mpeg/1.htmlに記載されている。そして、ｃ個に分割された部分コンテンツのそれぞれを識別、特定出来る、ｃ個の特定情報ＡＤＤＲ１、・・・、ＡＤＤＲｃを取得する。このｃ個の特定情報の取得方法としては、例えば、所定の方法で区切った部分コンテンツに対して順番に番号（例えば１、２、・・、ｃ）を付けていく方法や、部分コンテンツの先頭を表すアドレス（物理アドレスや論理アドレスなど）と部分コンテンツのサイズを計算する方法や、コンテンツの先頭からの経過時間を計算する方法などがある。ここでは、部分コンテンツＣＮＴ―１を識別、特定する情報を特定情報ＡＤＤＲ１、部分コンテンツＣＮＴ―２を識別、特定する情報を特定情報ＡＤＤＲ２、部分コンテンツＣＮＴ―３を識別、特定する情報を特定情報ＡＤＤＲ３、・・・、部分コンテンツＣＮＴ―ａを特定する情報を特定情報ＡＤＤＲａ、・・・、部分コンテンツＣＮＴ―ｃを特定する情報を特定情報ＡＤＤＲｃとする。そして、部分コンテンツと特定情報のｃ組｛ＣＮＴ―１、ＡＤＤＲ１｝、｛ＣＮＴ―２、ＡＤＤＲ２｝、・・・、｛ＣＮＴ―ａ、ＡＤＤＲａ｝、・・・、｛ＣＮＴ―ｃ、ＡＤＤＲｃ｝を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫと併せて、ヘッダ情報生成部４００６へ出力する。

【０１６５】

なお、例えば、コンテンツＣＮＴが２時間の動画データで各部分コンテンツが１秒の動画データの場合、ｃは７２００となるが、ｃは２以上の自然数であればどのような値でも良い。さらに、それぞれの特定情報は、上記で紹介した情報に限らず、各部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。さらには、上記情報を複数組み合わせた情報であっても良い。

【０１６６】

（６）ヘッダ情報生成部４００６

ヘッダ情報生成部４００６は、コンテンツ位置情報生成部４００５から、部分コンテンツと特定情報のｃ組｛ＣＮＴ―１、ＡＤＤＲ１｝、｛ＣＮＴ―２、ＡＤＤＲ２｝、・・・、｛ＣＮＴ―ａ、ＡＤＤＲａ｝、・・・、｛ＣＮＴ―ｃ、ＡＤＤＲｃ｝と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤを生成する。

【０１６７】

まず、ｃ組の部分コンテンツと特定情報の各組に対して、第一特定情報識別子を生成する。第一特定情報識別子を生成する方法としては、自然数を順番に割り当てていく（１、２、・・・、ｃ）方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した第一特定情報識別子をそれぞれ、ＡＤＤＲＩＤ１―１、ＡＤＤＲＩＤ１―２、・・・ＡＤＤＲＩＤ１―ａ、・・・、ＡＤＤＲＩＤ１―ｃとし、次のように第一特定情報識別子と部分コンテンツと特定情報とが対応しているとする。｛ＡＤＤＲＩＤ１―１、ＣＮＴ―１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ１―２、ＣＮＴ―２、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤ１―ａ、ＣＮＴ―ａ、ＡＤＤＲａ｝、・・・、｛ＡＤＤＲＩＤ１―ｃ、ＣＮＴ―ｃ、ＡＤＤＲｃ｝。続いて、ｃ組の第一特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値として第一ハッシュ値を計算する。部分コンテンツの第一ハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置４２の認証情報検証部４２７で用いる方法と同じものを用いる。ここで、各組に対して計算した第一ハッシュ値をそれぞれ、ＨＡＳＨ１―１、ＨＡＳＨ１―２、・・・、ＨＡＳＨ１―ａ、・・・、ＨＡＳＨ１―ｃとし、次のように第一特定情報識別子と部分コンテンツと特定情報と第一ハッシュ値が対応しているとする。｛ＡＤＤＲＩＤ１―１、ＣＮＴ―１、ＡＤＤＲ１、ＨＡＳＨ１―１｝、｛ＡＤＤＲＩＤ１―

２、ＣＮＴ－２、ＡＤＤＲ２、ＨＡＳＨ１－２｝、・・・、｛ＡＤＤＲＩＤ１－ａ、ＣＮＴ－ａ、ＡＤＤＲａ、ＨＡＳＨ１－ａ｝、・・・、｛ＡＤＤＲＩＤ１－ｃ、ＣＮＴ－ｃ、ＡＤＤＲｃ、ＨＡＳＨ１－ｃ｝。そして、その中から第一特定情報識別子と特定情報だけを抽出し、図４２で示すような、第一特定情報識別子と特定情報とからなるコンテンツ位置情報ＰＯＳ＝｛ＡＤＤＲＩＤ１－１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ１－２、ＡＤＤＲ２｝、・・・、｛ＡＤＤＲＩＤ１－ａ、ＡＤＤＲａ｝、・・・、｛ＡＤＤＲＩＤ１－ｃ、ＡＤＤＲｃ｝を生成する。

【０１６８】

続いて、ｃ組の第一特定情報識別子と部分コンテンツと特定情報と第一ハッシュ値を、ｅ個（ｅは１以上の自然数）のグループに分割する。ｅ個のグループに分割する方法は、例えば、システム（配布センタ４０及び実行装置４２）共通として与えられている数（例えば、ｃをｅで割った値以上で、ｃをｅで割った値に最も近い自然数。図４３では、５個ずつに分割している）毎に分割する方法や、配布センタ４０が外部から自然数を入力出来るようにして、その自然数毎に分割する方法などがある。なお、各ｅ個のグループに割り当てる数は、それぞれ異なる数であっても良い。そして、ｅ個のグループそれぞれに対して、第二特定情報識別子を生成する。第二特定情報識別子を生成する方法としては、例えば、そのグループに入っている第一特定情報識別子を羅列する方法などがある。なお、図４３のように、各グループにそれぞれ順番に並べられている場合、第二特定情報識別子は、それに入る第一特定情報識別子を全て羅列する必要はなく、最も若い第一特定情報識別子とそのグループに含まれる第一特定情報識別子の数だけから構成されるようにしても良い。さらに、予めｅ個のグループへの分割方法がシステム共通（配布センタ４０及び実行装置４２）として与えられている場合、第二特定情報識別子は、自然数を順番に割り当てていく（ｃ＋１、ｃ＋２、・・・、ｃ＋ｅ）方法や、乱数を用いてランダムに割り当てる方法などでもよい。ここで、各組に対して生成した第二特定情報識別子をそれぞれ、ＡＤＤＲＩＤ２－１、ＡＤＤＲＩＤ２－２、・・・、ＡＤＤＲＩＤ２－ｅとする。続いて、ｅ組の第二特定情報識別子の各組に対して、その第二特定情報識別子に含まれる一以上の第一特定情報識別子に対応する一以上の第一ハッシュ値を連結した値に対する属性値として第二ハッシュ値を計算する。一以上の第一ハッシュ値を連結した値に対する属性値を計算する方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置４２の認証情報検証部４２７で用いる方法と同じものを用いる。ここで、ｅ個のグループの各組に対して計算した第二ハッシュ値をそれぞれ、ＨＡＳＨ２－１、ＨＡＳＨ２－２、・・・、ＨＡＳＨ２－ｅとし、次のように第二特定情報識別子と第二ハッシュ値が対応しているとする。｛ＡＤＤＲＩＤ２－１、ＨＡＳＨ２－１｝、｛ＡＤＤＲＩＤ２－２、ＨＡＳＨ２－２｝、・・・、｛ＡＤＤＲＩＤ２－ｅ、ＨＡＳＨ２－ｅ｝。そして、ｃ組の第一特定情報識別子と部分コンテンツと特定情報と第一ハッシュ値から、第一特定情報識別子と第一ハッシュ値だけを抽出し、ｃ組の第一特定情報識別子と第一ハッシュ値、及び、ｅ組の第二特定情報識別子と第二ハッシュ値から構成される、図４４で示すような、ヘッダ情報ＨＥＡＤ＝｛ＡＤＤＲＩＤ１－１、ＨＡＳＨ１－１｝、｛ＡＤＤＲＩＤ１－２、ＨＡＳＨ１－２｝、・・・、｛ＡＤＤＲＩＤ１－ａ、ＨＡＳＨ１－ａ｝、・・・、｛ＡＤＤＲＩＤ１－ｃ、ＨＡＳＨ１－ｃ｝、｛ＡＤＤＲＩＤ２－１、ＨＡＳＨ２－１｝、・・・、｛ＡＤＤＲＩＤ２－ｅ、ＨＡＳＨ２－ｅ｝を生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部４００８へ出力する。

【０１６９】

（７）認証情報生成情報格納部４００７

認証情報生成情報格納部４００７は、ヘッダ情報ＨＥＡＤの認証情報である認証情報ＡＵＴＨを生成するための、認証情報生成情報ＧＥＮＡＵＴＨを予め与えられ、保持するものである。この認証情報生成情報ＧＥＮＡＵＴＨは、例えば、デジタル署名アルゴリズムの署名生成鍵（秘密鍵）である。認証情報生成情報ＧＥＮＡＵＴＨに対応する検証情報Ｖ

ＥＲは、実行装置３２の検証情報格納部３２５に格納されている。この検証情報ＶＥＲは、例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式やＲＳＡ署名などである。

【０１７０】

（８）認証情報生成部４００８

認証情報生成部４００８は、ヘッダ情報生成部４００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値に対する認証情報ＡＵＴＨを生成する。まず、認証情報生成情報格納部４００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値と認証情報生成情報ＧＥＮＡＵＴＨを用いて、ｅ個の第二ハッシュ値を連結した値に対する認証情報である認証情報ＡＵＴＨを生成する。なお、認証情報ＡＵＴＨの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズムを用いる方法の一例を、図４３を用いて説明する。まず、ヘッダ情報ＨＥＡＤに含まれるｅ個全ての第二ハッシュ値を結合した値ＨＡＳＨ２―１｜｜ＨＡＳＨ２―２｜｜・・・｜｜ＨＡＳＨ２―ｅに対する属性値（例：ハッシュ値）として、結合ハッシュ値＝ＯＷＦ（ＨＡＳＨ２―１｜｜ＨＡＳＨ２―２｜｜・・・｜｜ＨＡＳＨ２―ｅ）を生成する。そして、その結合ハッシュ値に対するデジタル署名を作成する。ここで、ＧＥＮＳＩＧ（Ｋ、Ｍ）を署名生成鍵Ｋを用いてメッセージＭに対して生成されたデジタル署名とすると、認証情報ＡＵＴＨは、ＡＵＴＨ＝ＧＥＮＳＩＧ（ＧＥＮＡＵＴＨ、ＯＷＦ（ＨＡＳＨ２―１｜｜ＨＡＳＨ２―２｜｜・・・｜｜ＨＡＳＨ２―ｅ））となる。ここで、ＯＷＦ（Ｘ）は、一方向性関数（例えば、ＳＨＡ－１アルゴリズム）にＸを入力した際の出力値とする。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部４００９へ出力する。なお、認証情報生成部４００８で使用するデジタル署名アルゴリズムは、実行装置４２の認証情報検証部４２７で用いるデジタル署名アルゴリズムと同じものを用いる。なお、認証情報生成部４００８では、認証情報ＡＵＴＨとして、結合ハッシュ値に対するデジタル署名を生成していたが、これに限るものではない。例えば、非特許文献１には、ＤＳＡ方式やＲＳＡ署名の動作として、署名対象メッセージに対するハッシュ関数（Ｈ）も含んでいる。このような場合、認証情報ＡＵＴＨは、結合ハッシュ値に対するデジタル署名ではなく、ｅ個全ての第二ハッシュ値を結合した値ＨＡＳＨ２―１｜｜ＨＡＳＨ２―２｜｜・・・｜｜ＨＡＳＨ２―ｅに対するデジタル署名でも良い。

【０１７１】

（９）暗号化部４００９

暗号化部４００９は、認証情報生成部４００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力された場合、以下のようにして暗号化コンテンツＥＮＣＣＮＴを生成する。コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。この暗号化コンテンツＥＮＣＣＮＴの生成方法としては、例えば、以下のような方法がある。まず、コンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ―１を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ―１＝Ｅｎｃ（ＣＫ、ＣＮＴ―１）を生成する。続いて、同じコンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ―２を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ―２＝Ｅｎｃ（ＣＫ、ＣＮＴ―２）を生成する。これを繰り返して、図４５で示すようなｃ個の暗号化部分コンテンツＥＮＣＣＮＴ―１、・・・、ＥＮＣＣＮＴ―ａ、・・・、ＥＮＣＣＮＴ―ｃから構成される暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを配布部４０１０へ出力する。暗号化部４００９で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置４２の部分復号化部４２５と同じ暗号アルゴリズム

を用いる。ここではＥＮＣＣＮＴの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵ＣＫで暗号化していたが、非特許文献１に記載のブロック暗号のモードを利用してもよい。例えば、ＣＢＣモードやＯＦＢモード、ＣＦＢモードなどでもよく、さらに、ある一定間隔毎にモード（例：ＣＢＣモード）の初期値を変化させるようにしたものでも良い。さらに、暗号化を行う単位は、コンテンツ位置情報生成部４００５でコンテンツＣＮＴを分割した単位に限るものではなく、例えば１６バイト毎であっても良い。

【０１７２】

（１０）配布部４０１０

配布部４０１０は、暗号化部４００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを可搬媒体４１へ記録するものである。例えば、可搬媒体４１が書き込み可能な光ディスクであり、配布部４０１０は書き込み用レーザー等を用いてデータを記録する。

【０１７３】

＜配布センタ４０の動作＞

以上で、配布センタ４０の構成について説明を行ったが、ここでは配布センタ４０の動作の一例について、図４６に示すフローチャートの処理を行う。なお、配布センタ４０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【０１７４】

入力部４００１は、外部から入力されたコンテンツＣＮＴをコンテンツ鍵生成部４００２へ出力し、コンテンツ鍵生成部４００２は、コンテンツ鍵ＣＫを生成し、コンテンツ鍵ＣＫ及びコンテンツＣＮＴを暗号化鍵束生成部４００４へ出力する（ステップＳ４０１）。

暗号化鍵束生成部４００４は、コンテンツ鍵生成部４００２からコンテンツ鍵ＣＫ及びコンテンツＣＮＴを入力され、実行装置情報格納部４００３にアクセスして複数の実行装置４２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。そして、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫをコンテンツ位置情報生成部４００５に出力する（ステップ４０２）。

【０１７５】

コンテンツ位置情報生成部４００５、暗号化鍵束生成部４００４から暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫを入力され、コンテンツＣＮＴをｃ個の部分コンテンツに分割し、そのｃ個の部分コンテンツのそれぞれを識別、特定するｃ個の特定情報を取得する。そして、ｃ組の部分コンテンツと特定情報を、暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとあわせて、ヘッダ情報生成部４００６へ出力する（ステップＳ４０３）。

【０１７６】

ヘッダ情報生成部４００６は、コンテンツ位置情報生成部４００５から、部分コンテンツと特定情報のｃ組｛ＣＮＴ－１、ＡＤＤＲ１｝、｛ＣＮＴ－２、ＡＤＤＲ２｝、・・・、｛ＣＮＴ－ａ、ＡＤＤＲａ｝、・・・、｛ＣＮＴ－ｃ、ＡＤＤＲｃ｝と暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力され、まず、ｃ組の部分コンテンツと特定情報の各組に対して、第一特定情報識別子を生成する。続いて、ｃ組の第一特定情報識別子と部分コンテンツと特定情報の各組に対して、部分コンテンツの属性値として第一ハッシュ値を計算する。そして、その中から第一特定情報識別子と特定情報だけを抽出し、第一特定情報識別子と特定情報とからなるコンテンツ位置情報ＰＯＳを生成する。続いて、ｃ組の第一特定情報識別子と部分コンテンツと特定情報と第一ハッシュ値を、ｅ個（ｅは１以上の自然数）のグループに分割する。そして、ｅ個のグループそれぞれに対して、第二特定情報識別子を生成する。続いて、ｅ組の第二特定情報識別子の各組に対して、その第二特定情報識別子に含まれる一以上の第一特定情報識別子に対応する一以上の第一ハッシュ値を連結した値に対する属性値として第二ハッシュ値を計算する。そして、ｃ組の

第一特定情報識別子と部分コンテンツと特定情報と第一ハッシュ値から、第一特定情報識別子と第一ハッシュ値だけを抽出し、ｃ組の第一特定情報識別子と第一ハッシュ値、及び、ｅ組の第二特定情報識別子と第二ハッシュ値から構成される、ヘッダ情報ＨＥＡＤを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫとを認証情報生成部４００８へ出力する（ステップＳ４０４）。

【０１７７】

認証情報生成部４００８は、ヘッダ情報生成部４００６からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢとコンテンツＣＮＴとコンテンツ鍵ＣＫが入力され、まず、認証情報生成情報格納部４００７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、ヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値と認証情報生成情報ＧＥＮＡＵＴＨを用いて、ｅ個の第二ハッシュ値を連結した値に対する認証情報である認証情報ＡＵＴＨを生成する。そして、コンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとを暗号化部４００９へ出力する（ステップＳ４０５）。

【０１７８】

暗号化部４００９は、認証情報生成部４００８からコンテンツ位置情報ＰＯＳとヘッダ情報ＨＥＡＤと暗号化鍵束ＫＢと認証情報ＡＵＴＨとコンテンツＣＮＴとコンテンツ鍵ＣＫとが入力される。そして、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを配布部４０１０へ出力する（ステップＳ４０６）。

【０１７９】

配布部４０１０は、暗号化部４００９から入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを可搬媒体４１へ記録する（ステップＳ４０７）。

以上が、不正コンテンツ検知システム４の構成要素である配布センタ４０の構成と動作である。続いて、可搬媒体４１の構成について説明を行う。

【０１８０】

＜可搬媒体４１の構成＞

可搬媒体４１は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のような光ディスクの媒体（メディア）であり、図４７に示すように、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが配布センタ４０によって記録されているものとする。

【０１８１】

以上が、不正コンテンツ検知システム４の構成要素である可搬媒体４１の構成である。続いて、実行装置４２の構成と動作について説明を行う。

＜実行装置４２の構成＞

実行装置４２は、図４８に示すように、取得部４２１、デバイス鍵格納部４２２、コンテンツ鍵取得部４２３、特定情報選択部４２４、部分復号化部４２５、検証情報格納部４２６、認証情報検証部４２７、実行部４２８とから構成される。

【０１８２】

（１）取得部４２１

取得部４２１は、可搬媒体４１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを取得する。そして、取得した暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ鍵取得部４２３へ出力する。

【０１８３】

（２）デバイス鍵格納部４２２

デバイス鍵格納部４２２は、配布センタ４０の実行装置情報格納部４００３の中の鍵情報の一部を保持するものであり、デバイス鍵格納部４２２に与えられる鍵情報と暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫが取得出来るものである。例えば、実行装置情報格納部４００３が図３９のような場合、デバイス鍵格納部４２２には、装置識別子ＡＩＤｉとデバイス鍵Ｋｉ（ｉは１からｎのいずれか）が与えられる。

【０１８４】

（３）コンテンツ鍵取得部４２３

コンテンツ鍵取得部４２３は、取得部４２１から暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、デバイス鍵格納部４２２に格納されている鍵情報及び暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫを取得する。例えば、暗号化鍵束ＫＢが図４０のような場合で、デバイス鍵格納部４２２には装置識別子ＡＩＤｉとデバイス鍵ＤＫｉ（ｉは１からｎのいずれか）が与えられている場合、コンテンツ鍵取得部４２３はデバイス鍵格納部４２２から装置識別子ＡＩＤｉとデバイス鍵ＤＫｉを取得し、暗号化鍵束ＫＢの中から装置識別子ＡＩＤｉに対応する暗号化コンテンツ鍵ＥＮＣＣＫｉ（ＥＮＣＣＫ１からＥＮＣＣＫｎの何れか）を取得する。そしてデバイス鍵ＤＫｉを基に、暗号化コンテンツ鍵ＥＮＣＣＫｉを復号化することによって、コンテンツ鍵ＣＫ＝Ｄｅｃ（ＤＪｉ、ＥＮＣＣＫｉ）を取得する。なお、Ｄｅｃ（Ｋ、Ｃ）を暗号文Ｃを復号化鍵Ｋを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを認証情報検証部３２５へ出力する。

【０１８５】

（４）特定情報選択部４２４

特定情報選択部４２４は、コンテンツ鍵取得部４２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、ヘッダ情報ＨＥＡＤに含むｃ個の第一特定情報識別子（ＰＯＳＩＤ１―１、・・・、ＰＯＳＩＤ１―ｃ）の中から、ｂ個の第一特定情報識別子（ｂは１以上ｃ－１以下の自然数）を選択する。ここでは、第三者によってどの第一特定情報識別子が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、特定情報選択部４２４が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献２が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、特定情報選択部４２４が温度センサや湿度センサを有することにより実現出来る。その後、選択されたｂ個の第一特定情報識別子と対応するｂ個の特定情報から成る被選択コンテンツ位置情報ＳＥＬＰＯＳを生成する。例として、図４９は、第一特定情報識別子ＡＤＤＲＩＤ１―２と特定情報ＡＤＤＲ２、第一特定情報識別子ＡＤＤＲＩＤ１―ａと特定情報ＡＤＤＲａを選択した場合の被選択コンテンツ位置情報ＳＥＬＰＯＳについて表している。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを部分復号化部４２５へ出力する。ここで、被選択コンテンツ位置情報ＳＥＬＰＯＳにはｂ組の第一特定情報識別子と特定情報を含むことになる。なお、パラメータｂは、システムパラメータ（全ての実行装置４２に予め共有に与えられているパラメータ）であってもよいし、各実行装置４２に個別に予め与えられているパラメータであってもよい。

【０１８６】

（５）部分復号化部４２５

部分復号化部４２５は、特定情報選択部４２４からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力された場合、以下の処理を行う。まず、被選択コンテンツ位置情報Ｓ

ＥＬＰＯＳの中の一組目の第一特定情報識別子と特定情報を抽出する。ここでは図４９の場合を例に挙げて、一組目の第一特定情報識別子と特定情報をそれぞれＡＤＤＲＩＤ１―２とＡＤＤＲ２とする。そして、暗号化コンテンツＥＮＣＣＮＴの中から特定情報ＡＤＤＲ２が特定する暗号化部分コンテンツＥＮＣＣＮＴ―２を取得し、コンテンツ鍵ＣＫを基に復号化を行い、部分コンテンツＣＮＴ―２を取得する（例えば、図５０参照）。続いて、被選択コンテンツ位置情報ＳＥＬＰＯＳの二組目以降の第一特定情報識別子と特定情報とを同様に抽出し、対応する部分コンテンツを取得する。そして、暗号化コンテンツＥＮＣＣＮＴと、ヘッダ情報ＨＥＡＤと、認証情報ＡＵＴＨと、抽出されたｂ組の第一特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、を検証情報検証部４２６へ出力する。なお、部分復号化部４２５で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式などであり、配布センタ４０の暗号化部４００９と同じ暗号アルゴリズムを用いる。

【０１８７】

（６）検証情報格納部４２６

検証情報格納部４２６は、ヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値に対する認証情報である認証情報ＡＵＴＨの正当性を検証するために必要な検証情報ＶＥＲを保持するものである。この検証情報ＶＥＲに対応する認証情報生成情報ＧＥＮＡＵＴＨは、配布センタ４０の認証情報生成情報格納部４００７に格納されている。例えば、検証情報ＶＥＲはデジタル署名アルゴリズムの署名検証鍵（公開鍵）である。

【０１８８】

（７）認証情報検証部４２７

認証情報検証部４２７は、部分復号化部４２５から、暗号化コンテンツＥＮＣＣＮＴと、認証情報ＡＵＴＨと、ヘッダ情報ＨＥＡＤと、ｂ組の第一特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、を入力する。そしてまず、図５１で示す一例のように、ｂ組の第一特定情報識別子と部分コンテンツに含まれるｂ個の部分コンテンツのそれぞれの属性値として、ハッシュ値を計算する（図５１における、黒色の第一ハッシュ値に対応）。部分コンテンツのハッシュ値を求める方法としては、例えば、一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、配布センタ４０のヘッダ情報生成部４００８で用いる方法と同じものを用いる。次に、ｂ組の第一特定情報識別子と部分コンテンツに含まれるｂ個の第一特定情報識別子において、そのｂ個の第一特定情報識別子のいずれか一つ以上を含んでいる第二特定情報識別子を取得する。これは、ｂ組の第一特定情報識別子と部分コンテンツに含まれるｂ個の部分コンテンツにおいて、そのｂ個の部分コンテンツのいずれか一つ以上含むデータに対する属性値である第二ハッシュ値（図５１における、黒色の第二ハッシュ値に対応）に対応する第二特定情報識別子と等しい。そして、その（一以上の）第二特定情報識別子に含まれる第一特定情報識別子であり、かつ、ｂ組の第一特定情報識別子と部分コンテンツに含まれない第一特定情報識別子を抽出し、その第一特定情報識別子に対応する第一ハッシュ値（図５１における、横線の第一ハッシュ値に対応）をヘッダ情報ＨＥＡＤから取得する。そして、ヘッダ情報ＨＥＡＤから取得した第一ハッシュ値とｂ個の部分コンテンツから計算されたｂ個のハッシュ値から、対応する第二ハッシュ値（図５１における、黒色の第二ハッシュ値に対応）を計算する。続いて、ｂ組の第一特定情報識別子と部分コンテンツにおいて、ｂ個の第一特定情報識別子のいずれの第一特定情報識別子も含んでいない第二特定情報識別子を抽出し、その第二特定情報識別子に対応する第二ハッシュ値（図５１における、横線の第二ハッシュ値に対応）をヘッダ情報ＨＥＡＤから取得する。そして、ｅ個の第二ハッシュ値を連結した値に対する属性値として、結合ハッシュ値を計算する。最後に、検証情報格納部４２６に格納されている検証情報ＶＥＲを使って、認証情報ＡＵＴＨが発行センタ４０によるヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正規の認証情報であるかを検証する。例えば、デジタル署名検証アルゴリズムを用いて、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正しいデジ

タル署名であるかを検証する。このデジタル署名検証アルゴリズムは、配布センタ４０の認証情報生成部４００８で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。認証情報検証部４２７は、認証情報ＡＵＴＨが発行センタ４０によるヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正しい認証情報である場合にのみ、コンテンツ鍵ＣＫと暗号化コンテンツＥＮＣＣＮＴを実行部４２８へ出力する。なお、ヘッダ情報ＨＥＡＤに含まれる第一ハッシュ値及び第二ハッシュ値の中で、認証情報検証部４２７において利用しない第一ハッシュ値及び第二ハッシュ値は、初めから取得部４２１で取得しないようにしても良い。これは、例えば、取得部４２１は、初めに、ヘッダ情報ＨＥＡＤを取得しないようにして、後ほど、認証情報検証部４２７において必要になった時に、必要な第一ハッシュ値及び第二ハッシュ値のみを取得するようにすることで実現出来る。

【０１８９】

（８）実行部４２８

実行部４２８は、認証情報検証部４２７から入力された暗号化コンテンツＥＮＣＣＮＴに含まれるｃ個の暗号化部分コンテンツＥＮＣＣＮＴ－１、・・・、ＥＮＣＣＮＴ－ｃを、コンテンツ鍵ＣＫを基に逐次復号化を行って部分コンテンツＣＮＴ－１、・・・、ＣＮＴ－ｃを取得し、逐次その部分コンテンツを実行するものである。例えば、実行部３２９はＭＰＥＧ２データやＭＰ３データをデコードする機能を有するデコータを有していて、ＭＰＥＧ２形式の動画コンテンツやＭＰ３形式の音声コンテンツであるコンテンツＣＮＴを逐次デコードして、外部に出力するようなものである。また、例えば、実行部３２９は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生するようなものでも良いし、別の可搬媒体や記録媒体にコンテンツデータを出力するようなものでも良いし、印刷機能を有しコンテンツデータを紙などに印刷するようなものでもよい。なお、復号化を行う単位やデコードを行う単位は、コンテンツ位置情報生成部４００５でコンテンツＣＮＴを分割した単位に限るものではなく、例えば１６バイト毎であっても良い。

【０１９０】

＜実行装置４２の動作＞

以上で、実行装置４２の構成について説明を行ったが、ここで実行装置４２の動作について、図５２に示すフローチャートを用いて説明する。なお、実行装置４２の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【０１９１】

取得部４２１は、可搬媒体４１に記録されているデータの読み取りを行い、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとをコンテンツ鍵取得部４２３へ出力する。そして、コンテンツ鍵取得部４２３は、入力された暗号化鍵束ＫＢ及びデバイス鍵格納部４２２が保持している鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを特定情報選択部４２４へ出力する（ステップＳ４２１）。

【０１９２】

特定情報選択部４２４は、コンテンツ鍵取得部４２３からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力され、ヘッダ情報ＨＥＡＤに含むｃ個の第一特定情報識別子（ＰＯＳＩＤ１－１、・・・、ＰＯＳＩＤ１－ｃ）の中から、ｂ個の第一特定情報識別子（ｂは１以上ｃ－１以下の自然数）を選択する。その後、選択されたｂ個の第一特定情報識別子と対応するｂ個の特定情報から成る被選択コンテンツ位置情報ＳＥＬＰＯＳを生成する。そして、コンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを部分復号化部４２５へ出力する（ステップＳ４２２）。

【０１９３】
部分復号化部４２５は、特定情報選択部４２４からコンテンツ鍵ＣＫとヘッダ情報ＨＥＡＤと被選択コンテンツ位置情報ＳＥＬＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが入力され、まず、被選択コンテンツ位置情報ＳＥＬＰＯＳの中の一組目の第一特定情報識別子と特定情報を抽出する。そして、暗号化コンテンツＥＮＣＣＮＴの中から暗号化部分コンテンツを取得し、コンテンツ鍵ＣＫを基に復号化を行い、部分コンテンツを取得する。続いて、被選択コンテンツ位置情報ＳＥＬＰＯＳの二組目以降の第一特定情報識別子と特定情報とを同様に抽出し、対応する部分コンテンツを取得する。そして、暗号化コンテンツＥＮＣＣＮＴと、ヘッダ情報ＨＥＡＤと、認証情報ＡＵＴＨと、抽出されたｂ組の第一特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、を検証情報検証部４２６へ出力する（ステップＳ４２３）。
【０１９４】
認証情報検証部４２７は、部分復号化部４２５から、暗号化コンテンツＥＮＣＣＮＴと、認証情報ＡＵＴＨと、ヘッダ情報ＨＥＡＤと、ｂ組の第一特定情報識別子と部分コンテンツと、コンテンツ鍵ＣＫと、を入力する。そしてまず、ｂ組の第一特定情報識別子と部分コンテンツに含まれるｂ個の部分コンテンツのそれぞれの属性値として、ハッシュ値を計算する。次に、ｂ組の第一特定情報識別子と部分コンテンツに含まれるｂ個の第一特定情報識別子において、そのｂ個の第一特定情報識別子のいずれか一つ以上を含んでいる第二特定情報識別子を取得する。そして、その（一以上の）第二特定情報識別子に含まれる第一特定情報識別子であり、かつ、ｂ組の第一特定情報識別子と部分コンテンツに含まれない第一特定情報識別子を抽出し、その第一特定情報識別子に対応する第一ハッシュ値をヘッダ情報ＨＥＡＤから取得する。そして、ヘッダ情報ＨＥＡＤから取得した第一ハッシュ値とｂ個の部分コンテンツから計算されたｂ個のハッシュ値から、対応する第二ハッシュ値を計算する。続いて、ｂ組の第一特定情報識別子と部分コンテンツにおいて、ｂ個の第一特定情報識別子のいずれの第一特定情報識別子も含んでいない第二特定情報識別子を抽出し、その第二特定情報識別子に対応する第二ハッシュ値をヘッダ情報ＨＥＡＤから取得する。そして、ｅ個の第二ハッシュ値を連結した値に対する属性値として、結合ハッシュ値を計算する。最後に、検証情報格納部４２６に格納されている検証情報ＶＥＲを使って、認証情報ＡＵＴＨが発行センタ４０によるヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正規の認証情報であるかを検証する（ステップＳ４２４）。
【０１９５】
認証情報検証部４２７は、認証情報ＡＵＴＨが発行センタ４０によるヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正しい認証情報である場合にのみ、コンテンツ鍵ＣＫと暗号化コンテンツＥＮＣＣＮＴを実行部４２８へ出力し、ステップＳ４２６へ進む。もし、認証情報ＡＵＴＨがヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値（結合ハッシュ値）に対する正しい認証情報ではない場合、処理を終了する（ステップＳ４２５）。
【０１９６】
実行部４２８は、認証情報検証部４２７から受け取った暗号化コンテンツＥＮＣＣＮＴの中の暗号化部分コンテンツを、コンテンツ鍵を用いて逐次復号化し、その部分コンテンツを実行する（ステップＳ４２６）。
以上が、不正コンテンツ検知システム４の構成要素である実行装置４２の構成と動作である。尚、コンテンツ鍵取得部４２３、特定情報選択部４２４、認証情報検証部４２７、等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。
【０１９７】
ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ Ｐｒｏｇｒａｍｍａｂｌｅ Ｇａｔｅ Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

【０１９８】

さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

＜不正コンテンツ検知システム４の効果＞

以上、不正コンテンツ検知システム４について実施の形態に基づいて説明したが、この不正コンテンツ検知システム４においては、不正コンテンツ検知システム３と同様に、ヘッダ情報ＨＥＡＤに含まれるｃ個のハッシュ値のうち、ｂ個のハッシュ値に絞って検証するようにすることで、検証に要する処理時間を短縮することが出来る。また、これは、コンテンツＣＮＴを実行、再生開始する毎に、毎回異なるハッシュ値を検証するようにすることで、コンテンツＣＮＴの一部分もしくは全部を不正な部分コンテンツに差し替えた場合、ある確率でコンテンツＣＮＴを実行できなくなることになる。これにより、コンテンツＣＮＴの中の一部分もしくは全部を、不正なコンテンツに差し替えられた不正コンテンツ（海賊版コンテンツ）等の流通に対する抑止力となる。

【０１９９】

また、実施の形態３で説明した不正コンテンツ検知システム３における実行装置３２では、可搬媒体３１からｃ個のハッシュ値を全て取得しないといけなかったが（図３２参照）、本実施形態の実行装置４２では、可搬媒体４１からｃ個の第一ハッシュ値の一部と、ｅ個の第二ハッシュ値の一部のみだけを取得すればよくなった。これにより、実行装置４２は、実行装置３２に比べ、可搬媒体から取得しなくてはならないハッシュ値（実施の形態４では第一ハッシュ値と第二ハッシュ値の合計、実施の形態３ではハッシュ値）の数を少なくすることが出来、処理時間を短くすることが出来た。

【０２００】

さらに、実施の形態３で説明した不正コンテンツ検知システム３における実行装置３２では、認証情報検証部３２５及びヘッダ情報検証部３２８でそれぞれ検証処理（計２回）を行っていたが、本実施形態の実行装置４２では、認証情報検証部４２７でのみ検証処理（１回）を行うようにした。これにより、実行装置４２は、実行装置３２に比べ、検証処理における処理時間を短くすることが出来た。

【０２０１】

さらに、実行装置４２は、認証情報ＡＵＴＨの正当性の検証を、コンテンツＣＮＴを実行、再生開始する前に全て行うため、コンテンツＣＮＴの実行、再生中の特別な処理が必要なくなり、従来例に比べ、コンテンツＣＮＴの実行中の処理負荷が軽減されるという効果を有する。

＜変形例＞

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０２０２】

（１）実施の形態１において、認証情報ＡＵＴＨは、ヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値に対する認証情報（例：デジタル署名）であったが、実行装置１２においてヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値の正当性を検証出来るものであれば、どのようなものでも良い。例えば、デジタル署名方式を用いずにＡＥＳなどの秘密鍵暗号を用いても同様のことが実現出来る。まず、認証情報生成情報格納部１００７及び検証情報格納部１２５には、同じ鍵Ｋが与えられているとする。そして、認証情報生成部１００８では、鍵Ｋを用いてヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値を暗号化した暗号文を認証情報ＡＵＴＨとする。（なお、ｋ個のハ

ッシュ値を連結した値を入力とした場合の一方向性関数の出力値を暗号化しても良い）。認証情報検証部１２６では、鍵Ｋを用いて入力された認証情報ＡＵＴＨを復号化し、その復号結果がヘッダ情報ＨＥＡＤと一致していてば、認証情報ＡＵＴＨは正当であると判断する。このようにして、デジタル署名アルゴリズムを使用しなくても、ヘッダ情報の正当性を検証することが出来る。同様に、一方向性関数や鍵付き一方向性関数などを用いても同様に実現出来る。なお、実施の形態２においても、同様にデジタル署名アルゴリズムの替わりに、ＡＥＳなどの秘密鍵暗号や一方向性関数や鍵付き一方向性関数などを利用出来る。

【０２０３】

（２）実施の形態１の可搬媒体１１では、暗号化コンテンツ位置情報ＥＮＣＰＯＳが記録されていたが、図５３のように、可搬媒体１１には、暗号化されていないコンテンツ位置情報ＰＯＳをそのまま記録するようにしても良い。こうすることにより、実行装置１２で暗号化コンテンツ位置情報ＥＮＣＰＯＳを復号化する必要がなくなる。なお、実施の形態２においても、同様のことが実現出来る。

【０２０４】

（３）実施の形態１の可搬媒体１１に記録される認証情報ＡＵＴＨは、ヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値に対する配布センタ１０の認証情報（例：デジタル署名）であったが、ｋ個（ｋは１以上の自然数）の代表部分コンテンツＰ１―ＣＮＴ、・・・、Ｐｋ―ＣＮＴを連結した値に対する配布センタ１０のデジタル署名であっても良い。

【０２０５】

これは、可搬媒体１１には、図５４で示すように、ヘッダ情報ＨＥＡＤと認証情報ＡＵＴＨの替わりに、コンテンツ認証情報ＣＮＴＡＵＴＨを記録するようにし、コンテンツ認証情報ＣＮＴＡＵＴＨが、図５５で示すように、特定情報識別子とその特定情報識別子に対応する代表部分コンテンツのデジタル署名のｋ組から成り、さらに、実行装置１２の認証情報検証部１２６では、ヘッダ情報ＨＥＡＤに含まれるｋ個のハッシュ値を連結した値に対する認証情報ＡＵＴＨの正当性を検証するのではなく、特定情報識別子に対応する代表部分コンテンツに対するデジタル署名（Ｓ１、・・・、Ｓｋ）の正当性を検証するようにすることによって、実現出来る。

【０２０６】

また、別の実現方法としては、コンテンツ認証情報ＣＮＴＡＵＴＨは、図５５で示すように、各特定情報識別子に対応する代表部分コンテンツのそれぞれのデジタル署名を含んでいなくてもよく、図５６で示すように、各特定情報識別子に対応する代表部分コンテンツを連結した一つの値に対するデジタル署名ＳＩＧを一つ含んでいてもよい。（なお、ここで、一方向性関数を用いて、代表部分コンテンツを連結した一つの値のデータサイズを小さくしても良い）

こうすることにより、可搬媒体１１にヘッダ情報ＨＥＡＤを記録しなくてすむため、記録データのサイズを削減することが出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２０７】

（４）実施の形態１の可搬媒体１１には、暗号化コンテンツ位置情報ＥＮＣＰＯＳが記録されていたが、図５７のように、可搬媒体１１には、暗号化コンテンツ位置情報ＥＮＣＰＯＳを記録せずに、実行装置１２のコンテンツ位置情報格納部に暗号化コンテンツ位置情報ＥＮＣＰＯＳを保持するようにして、コンテンツ位置情報取得部１２４は、コンテンツ位置情報格納部にアクセスして、暗号化コンテンツ位置情報ＥＮＣＰＯＳを取得するようにしてもよい。

【０２０８】

また、可搬媒体１１にはさらに、図５８で示すように、コンテンツ位置情報ＰＯＳを識別するコンテンツ位置情報識別子ＣＮＴＡＩＤｉ（ＣＮＴＡＩＤ１、・・・、ＣＮＴＡＩＤｇのいずれか、ｇは１以上の自然数）が記録されており、実行装置１２のコンテンツ位

置情報格納部は、コンテンツ位置情報識別子ＣＮＴＡＩＤ１、・・・、ＣＮＴＡＩＤｇのそれぞれに対応する暗号化コンテンツ位置情報ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｇを保持しており、コンテンツ位置情報取得部１２４は、コンテンツ位置情報格納部にアクセスして、コンテンツ位置情報識別子ＣＮＴＡＩＤｉに対応する暗号化コンテンツ位置情報ＥＮＣＰＯＳｉ（ＥＮＣＰＯＳ１、・・・、ＥＮＣＰＯＳｇのいずれか）を取得するようにしてもよい。

【０２０９】

こうすることにより、可搬媒体１１に暗号化コンテンツ位置情報ＥＮＣＰＯＳを記録する必要がなくなるため、記録データのサイズを削減することが出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

なお、変形例（２）と組み合わせて、実行装置１２のコンテンツ位置情報格納部には、暗号化コンテンツ位置情報ＥＮＣＰＯＳではなく、暗号化されていないコンテンツ位置情報ＰＯＳをそのまま格納しても良い。なお、これも、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２１０】

（５）実施の形態１の認証情報ＡＵＴＨは、図８のように、ｋ個のハッシュ値を連結した値に対する認証情報であったが、これに限るものではない。例えば、ｋ個の特定情報識別子とｋ個のハッシュ値を連結した値であっても良い。さらに、図５９のように、ｋ個のハッシュ値に加え、コンテンツ鍵ＣＫを連結した値に対する認証情報であっても良い。この場合、可搬媒体１１に記録するヘッダ情報としては、図８のように、ｋ組の特定情報識別子とハッシュ値のみにする。こうすることにより、コンテンツ鍵ＣＫを持たないものは、認証情報ＡＵＴＨの正当性すら検証出来なくなり、安全性がより高まる。なお、コンテンツ鍵ＣＫではなく、ハッシュ値の数、などでもよい。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２１１】

（６）実施の形態１の認証情報ＡＵＴＨは、図８のように、ｋ個のハッシュ値を連結した値に対する認証情報であったが、図６０のように、ｋ個のハッシュ値に加え、コンテンツＣＮＴのサイズであるコンテンツサイズＣＮＴＳＩＺＥを連結した値に対する認証情報であっても良い。こうすることにより、コンテンツＣＮＴのサイズも認証情報ＡＵＴＨに影響するため、安全性がより高まる。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２１２】

（７）実施の形態２の実行装置２２の取得部２２１では、ｍ種類のヘッダ識別子のうち、１種類のヘッダ識別子のみを選択していたが、１種類ではなく、ｓ種類（ｓは２以上ｍ以下の自然数）のヘッダ識別子を選択し、ｓ種類のヘッダ情報と認証情報の正当性を検証するようにしてもよい。こうすることにより、ヘッダ情報と認証情報の正当性検証を一度にｓ回行うことが出来、処理時間は多くかかるが、安全性を向上させることが出来る。

【０２１３】

（８）実施の形態１の可搬媒体１１では、暗号化コンテンツＥＮＣＣＮＴが記録されていたが、可搬媒体１１には、暗号化されていないコンテンツＣＮＴをそのまま記録するようにしても良い。こうすることにより、実行装置１２で暗号化コンテンツＥＮＣＣＮＴを復号化する必要がなくなる。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２１４】

（９）実施の形態１の配布センタ１０は、図２で示すような構成に限るものではない。例えば、認証情報ＡＵＴＨなどを可搬媒体１１へ記録する配布部１０１０と、ヘッダ情報ＨＥＡＤに対する認証情報を生成する認証情報生成部１００８とを、別の主体が行うようにしても良い。例えば、コンテンツＣＮＴに対する認証情報を生成するのはコンテンツＣＮＴの正規の著作権者であり、認証情報ＡＵＴＨなどを可搬媒体１１へ記録するのはディスク製造業者であるなど、が考えられる。なお、実施の形態２及び実施の形態３及び実施

の形態４においても、同様のことが実現出来る。

【０２１５】

（１０）実施の形態１の配布センタ１０の認証情報生成情報格納部１００７、及び、実行装置１２の検証情報格納部１２５は、これに限るものではない。例えば、以下のような例が考えられる。

（ｉ）一つの例として、認証情報生成情報格納部１００７は、図６１で示すように、１つの認証情報生成情報ＧＥＮＡＵＴＨｉ（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗのいずれか　ｗは１以上の自然数）と対応する検証情報識別子ＶＥＲＩＤｉを保持しており、検証情報格納部１２５は、図６２で示すように、ｗ組の検証情報識別子（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗ）と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報（ＶＥＲ１、・・・、ＶＥＲｗ）を保持している場合が考えられる。この場合、配布センタ１０の配布部１０１０は、可搬媒体１１に、認証情報生成情報格納部１００７に格納されている検証情報識別子ＧＥＮＡＵＴＨｉを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、可搬媒体１１に記録されている検証情報識別子ＧＥＮＡＵＴＨｉに対応する検証情報ＶＥＲｉ（ＶＥＲ１、・・・、ＶＥＲｗのいずれか）を検証情報格納部１２５から取得し、その検証情報ＶＥＲｉを基に、認証情報ＡＵＴＨを検証することになる。

【０２１６】

（ｉｉ）別の例として、認証情報生成情報格納部１００７には、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲを保持しており、検証情報格納部１２５には、何も保持してない場合が考えられる。この場合、配布センタ１０の配布部１０１０は、可搬媒体１１に、認証情報生成情報格納部１００７に格納されている検証情報ＶＥＲを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、可搬媒体１１に記録されている検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証することになる。

【０２１７】

（ｉｉｉ）さらなる別の例として、認証情報生成情報格納部１００７には、図６３で示すように、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲ、及び、第三者機関によって生成された検証情報ＶＥＲに対する認証情報（例えばセンタによるデジタル署名）であるセンタ認証情報ＣＡＵＴＨを保持しており、検証情報格納部１２５は、図６４で示すように、第三者機関の検証情報であるセンタ検証情報ＣＶＥＲ（例えばセンタのデジタル署名の署名検証鍵）を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）や、鍵配布センタなどである。この場合、配布センタ１０の配布部１０１０は、可搬媒体１１に、認証情報生成情報格納部１００７に格納されている検証情報ＶＥＲ及びセンタ認証情報ＣＡＵＴＨを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、検証情報格納部１２５のセンタ検証情報ＣＶＥＲを用いて、可搬媒体１１に記録されているセンタ認証情報ＣＡＵＴＨが、検証情報ＶＥＲに対する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証するようにすることになる。

【０２１８】

このようにすることによって、配布センタ１０が複数存在している場合にそれぞれの配布センタ１０に別の検証情報を設定したとしても、実行装置１２に予め各検証情報を保持しておく必要がなくなる。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

（１１）変形例（１０）において、実行装置１２は、さらに、無効検証情報を外部から受信するようにしてもよい。例えば、変形例１１の（ｉ）の場合、無効検証情報には、検証情報識別子が含まれており、実行装置１２には、外部から無効検証情報として検証情報識別子ＧＥＮＡＵＴＨｊを受信した場合に、検証情報格納部１２５に格納されている検証情報識別子ＧＥＮＡＵＴＨｊに対応する検証情報ＶＥＲｊを無効化する検証情報無効化部を備えていてもよい。

【０２１９】
また、変形例（１０）の（ｉｉ）及び（ｉｉｉ）の場合、無効検証情報には、検証情報が含まれており、実行装置１２の検証情報格納部１２５は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部１２６は、検証情報格納部１２５の無効検証情報に、可搬媒体１１に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツＣＮＴの実行開始を行わないようにしてもよい。
【０２２０】
なお、実行装置１２が外部から無効検証情報を受信する方法としては、可搬媒体１１や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。このようにすることによって、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。
【０２２１】
（１２）変形例（１１）において、実行装置１２は、最新の無効検証情報のみを検証情報格納部１２５に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置１２は、検証情報格納部１２５が保持する無効検証情報よりも発効日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２５に上書きするようにしてもよいし、また、無効検証情報には発行ＩＤが記載されており、実行装置１２は、検証情報格納部１２５が保持する無効検証情報よりも発行ＩＤが最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２５に上書きするようにしてもよい。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。
【０２２２】
（１３）実施の形態１のコンテンツＣＮＴは、動画データや音声データなどのコンテンツであったが、コンピュータプログラムであっても良い。この場合、実行装置１２は、コンピュータプログラムを実行するために必要なＣＰＵやメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置１２では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。
【０２２３】
（１４）実施の形態１の配布センタ１０では、コンテンツ位置情報生成部１００５においてコンテンツＣＮＴに対するコンテンツ位置情報ＰＯＳを生成していたが、配布センタ１０が一以上のコンテンツ位置情報ＰＯＳを保持するコンテンツ位置情報格納部を有していて、コンテンツ位置情報生成部１００５はコンテンツ位置情報格納部からいずれかのコンテンツ位置情報ＰＯＳを取得するようにしても良い。こうすることにより、コンテンツ位置情報ＰＯＳを予めまとめて作成しておくことが出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。
【０２２４】
（１５）実施の形態１の配布センタ１０では、コンテンツ鍵生成部１００２においてコンテンツ鍵ＣＫを生成していたが、配布センタ１０が一以上のコンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵生成部１００２はコンテンツ鍵格納部からいずれかのコンテンツ鍵ＣＫを取得するようにしても良い。こうすることにより、コンテンツ鍵ＣＫを予めまとめて作成しておくことが出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。
【０２２５】
（１６）実施の形態１の実行装置１２のコンテンツ鍵取得部１２３では、暗号化鍵束ＫＢ、及びデバイス鍵格納部１２２に格納されている情報を用いて、コンテンツ鍵ＣＫを取

得していたが、配布センタ１０がデバイス鍵格納部１２２の替わりに、コンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部１２３はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ１０は可搬媒体１１に暗号化鍵束ＫＢを記録する必要はなく、実行装置１２は暗号化鍵束ＫＢを受信する必要もない。こうすることにより、可搬媒体１１に暗号化鍵束ＫＢを記録しなくてすむため、記録データのサイズを削減することが出来る。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２２６】

（１７）実施の形態１において、配布センタ１０は、可搬媒体１１を介して実行装置１２へコンテンツＣＮＴに関する情報を配布していたが、これに限るものではない。例えば、配布センタ１０と実行装置１２がインターネット等の通信ネットワークに接続されており、配布センタ１０は、その通信ネットワークを介して実行装置１２へコンテンツＣＮＴに関する情報を配布してもよいし、他にも通信ネットワークが放送網であってもよい。なお、実施の形態２及び実施の形態３及び実施の形態４においても、同様のことが実現出来る。

【０２２７】

（１８）実施の形態３において、実行装置３２は可搬媒体３１内のコンテンツＣＮＴを実行開始する前に、そのコンテンツＣＮＴが不正なものであるか検証していたが、それに限るものではない。例えば、可搬媒体３１が光ディスクであり、実行装置３２がディスクトレイを有している場合、可搬媒体３１が実行装置３２のディスクトレイに挿入された場合に、そのコンテンツＣＮＴが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体３１内のコンテンツＣＮＴをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時１度しか検証しないですむようになるため、コンテンツＣＮＴの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体３１がＳＤカード等の外部メモリで、実行装置３２が外部メモリスロットを有している場合にも、同様のことが実現出来る。また、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２２８】

（１９）実施の形態３において、配布センタ３０は、可搬媒体３１にヘッダ情報ＨＥＡＤを記録するようにしていたが、可搬媒体３１にヘッダ情報ＨＥＡＤを記録しないようにしても良い。これは、例えば、実行装置３２は、選択された部分コンテンツから計算されるハッシュ値が、ヘッダ情報ＨＥＡＤに含まれるハッシュ値と一致しているか検証する代わりに、図６５で示すように、部分コンテンツを基にハッシュ値を生成し、それらハッシュ値からヘッダ情報ＨＥＡＤを生成し、可搬媒体３１に記録されている認証情報ＡＵＴＨが生成したヘッダ情報ＨＥＡＤに対する正規の認証情報（例えばデジタル署名）であるか検証することで実現できる。こうすることにより、可搬媒体３１に記録するデータサイズを小さくすることが出来る。なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２２９】

（２０）実施の形態３において、実行装置３２は、選択された部分コンテンツから計算されるハッシュ値が、ヘッダ情報ＨＥＡＤに含まれるハッシュ値に一致しているか検証していたが、これに限るものではない。例えば、実施の形態４で利用しているテクニックを実施の形態３に適用することが出来る。図６６で示すように、実行装置３２は、選択された部分コンテンツからハッシュ値を計算し、その計算したハッシュ値を可搬媒体３１に記録されているヘッダ情報ＨＥＡＤの対応するハッシュ値と入れ替え、図６７で示すように、第二ヘッダ情報ＨＥＡＤｘを生成する。そして、可搬媒体３１に記録されている認証情報ＡＵＴＨが第二ヘッダ情報ＨＥＡＤｘの正規の認証情報（例えばデジタル署名）であるか検証するようにしてもよい。こうすることにより、実行装置３２において、ハッシュ値が一致しているか検証する必要がなくなり、計算量の削減が実現出来る。なお、実施の形態１及び実施の形態２においても、同様のことが実現出来る。

【０２３０】
（２１）実施の形態３のコンテンツ位置情報生成部３００５において、図６８のように、外部から要求情報ＲＥＱを受信するようにして、その要求情報ＲＥＱを基にコンテンツＣＮＴを分割するようにしても良い。この要求情報ＲＥＱは、コンテンツＣＮＴを区切るための情報であり、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位、１秒単位といった情報である。これは、例えば、コンテンツ位置情報生成部３００５がキーボードやマウスと接続されていることにより実現できる。さらに、それぞれの部分コンテンツのサイズ（分割単位）は、全て同じである必要はない、それぞれ異なっていても良い。また、コンテンツを分割する数（ｃ）は、コンテンツＣＮＴに応じて変えても良い。
【０２３１】
また、コンテンツを分割する単位は、システム共通のパラメータとして与えられていても良い。この場合、可搬媒体３１にはコンテンツ位置情報ＰＯＳを格納しておく必要はない。なお、実施の形態４においても、同様のことが実現出来る。
（２２）実施の形態３において、可搬媒体３１にはヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴとをそれぞれ一つずつ格納していたが、これに限るものではない。例えば、図６９で示すように、可搬媒体３１にはヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと暗号化コンテンツＥＮＣＣＮＴをそれぞれｚ個（ｚは２以上の自然数）格納しても良い。このような場合、以下のようなことが実現出来る。ここでは、例えば、可搬媒体３１が光ディスクであり、実行装置３２はディスクトレイを有しているとする。この場合、可搬媒体３１が実行装置３２のディスクトレイに挿入された時に、複数のコンテンツを構成する全ての部分コンテンツの中からｒ個の部分コンテンツを選択しそのハッシュ値を計算し、そのｒ個（ｒは１以上の自然数）のハッシュ値がヘッダ情報の中のハッシュ値と一致しているかどうかを行うようにする。そして、複数あるコンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツを構成する部分コンテンツの中からｄ個（ｄは１以上ｒ－１以下の自然数）の部分コンテンツを選択しそのハッシュ値を計算し、ヘッダ情報に含まれるハッシュ値と一致しているか検証を行うようにしても良い。つまり、可搬媒体３１が実行装置３２のディスクトレイに挿入された場合に一度のみ、ある程度の数のハッシュ値の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数のハッシュ値を検証するようにする。これにより、ディスクトレイに挿入された可搬媒体３１内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体３１は光ディスク出なくてもよく、例えばＳＤカード等の外部メモリであっても同様のことが実現出来る。また、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。
【０２３２】
（２３）実施の形態３において、各ハッシュ値（ＨＡＳＨ１、・・・、ＨＡＳＨｃ）は、部分コンテンツに対する属性値（ハッシュ値）であったが、これに限るものではない。例えば、部分コンテンツと特定情報（例えば物理アドレスなど）を連結した値に対する属性値（ハッシュ値）であってもよい。これにより、コンテンツＣＮＴの中のある部分コンテンツを不正な部分コンテンツに差し替えようとする攻撃に対する安全性をより向上させることが出来る。なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。
【０２３３】
（２４）実施の形態３においては、実行装置３２の認証情報検証部３２５及びヘッダ情報検証部３２８における検証結果の両方、もしくは、いずれかが不正である場合、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するようにしていたが、これに限るものではない。例えば、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するに加え、実行部３２９では、実行、再生が禁止されている旨、外部に出力（例えば、ディスプレイに「不正なコンテンツです」と表示する）するようにしても良い。また、暗

号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するのではなく、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生は行うが、同時に外部に警告を出力（例えば、ディスプレイに「警告：不正なコンテンツです」と表示する）するようにしても良い。また、さらに、実行装置３２とサーバ（配布センタ３２や別のセンタ）とが通信ネットワーク等で接続されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。また、さらに、実行装置３２では以後、あらゆる暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するようにしてもよい。また、さらに、実行装置３２は、不正コンテンツを識別するコンテンツ識別情報（例えば、コンテンツ識別子）を装置内に記録するようにして、一定期間内、もしくは、永久的に、コンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、さらに、可搬媒体３１が光ディスクであり、実行装置３２がディスクトレイを有している場合、可搬媒体３１がディスクトレイから排出されるようにしても良い。なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２３４】

（２５）実施の形態３の可搬媒体３１には、コンテンツ位置情報ＰＯＳが記録されていたが、これに限るものではない。例えば、図７０のように、可搬媒体３１には、暗号化されたコンテンツ位置情報ＰＯＳを記録するようにしても良い。ここで用いる鍵は、例えば、コンテンツ鍵ＣＫなどが利用可能である。これにより、鍵を知らない者はコンテンツ位置情報ＰＯＳを取得出来なくなるため、コンテンツＣＮＴの中のある部分コンテンツを不正な部分コンテンツに差し替えようとする攻撃に対する安全性をより向上させることが出来る。なお、実施の形態４においても、同様のことが実現出来る。

【０２３５】

（２６）実施の形態３において、実行装置３２の取得部３２１は、可搬媒体３１から暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを一度に取得していたが、これに限るものではない。例えば、取得部３２１は可搬媒体３１から、初めに暗号化鍵束ＫＢだけを取得し、コンテンツ鍵取得部３２３の処理を行う。そして、認証情報検証部３２５は、初めに、取得部３２１経由で、可搬媒体３１からヘッダ情報ＨＥＡＤと認証情報ＡＵＴＨを取得してから、認証情報検証部の処理を行う。その検証が成功した場合に、特定情報選択部３２６は、取得部３２１経由で、可搬媒体３１からコンテンツ位置情報ＰＯＳを取得してから、特定情報選択部３２６の処理を行う。そして、部分復号化部３２７は、取得部３２１経由で、可搬媒体３１から、特定情報選択部３２６で選択された特定情報に対応する暗号化部分コンテンツを取得してから、部分復号化部３２７及びヘッダ情報検証部３２８の処理を行う。そして、ヘッダ情報検証部３２８での検証が成功した場合に、実行部３２９は、取得部３２１経由で、可搬媒体３１から暗号化コンテンツＥＮＣＣＮＴ（もしくは、部分復号化部３２７で取得された暗号化部分コンテンツ以外の暗号化部分コンテンツ）を逐次取得し、実行部３２９の処理を行うようにしても良い。そうすることにより、可搬媒体３１内に不正な認証情報、もしくは、不正なヘッダ情報が記録されている場合には、実行装置３２は暗号化コンテンツＥＮＣＣＮＴを取得しないようになるため、実行装置の処理負荷が軽減されるという利点が生まれる。なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２３６】

（２７）実施形態３において、実行装置３２の部分復号化部３２７は、初めに、被選択コンテンツ位置情報ＳＥＬＰＯＳに含まれる一組目の特定情報識別子と特定情報を抽出し、暗号化コンテンツＥＮＣＣＮＴの中からその一組目の特定情報に対応する暗号化部分コンテンツを取得するようにしていたが、これに限るものではない。例えば、部分復号化部３２７は、アクセス時間の高速化を目的に、暗号化コンテンツＥＮＣＣＮＴの中から暗号化部分コンテンツを取得する前に、被選択コンテンツ位置情報ＳＥＬＰＯＳの中の特定情報識別子と特定情報の組のそれぞれに取得順序情報を付加した高速化被選択コンテンツ位置情報ＦＳＥＬＰＯＳを生成して、その高速化被選択コンテンツ位置情報ＦＳＥＬＰＯＳ

を基に、暗号化コンテンツＥＮＣＣＮＴの中から暗号化部分コンテンツを順番に取得するようにしても良い。

【０２３７】

ここでは一例として、以下のような状況を想定する。まず、図７１で示すように、被選択コンテンツ位置情報ＳＥＬＰＯＳは、４組の特定情報識別子と特定情報（｛ＡＤＤＲＩＤ４、ＡＤＤＲ４｝、｛ＡＤＤＲＩＤ２、ＡＤＤＲ２｝、｛ＡＤＤＲＩＤ１、ＡＤＤＲ１｝、｛ＡＤＤＲＩＤ３、ＡＤＤＲ３｝）から構成しているとする。可搬媒体３２は、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの光ディスクであるとする。その可搬媒体３２（光ディスク）上には、データを記録する部分がいくつかに分かれており、年輪状に広がっている各領域をトラックと呼ぶ。各トラックには、いくつかのセクタを含み、データはセクタ単位で読み書きされる。例えば、１セクタのサイズは５１２バイトである。このような場合、可搬媒体３２上の読み取り対象データは、トラック識別番号やセクタ識別番号やセクタサイズにより特定することが出来る。取得部３２１は、ヘッド機構部（ピックアップ）及び回転軸を備え、回転軸により可搬媒体３１（光ディスク）を半時計回りに回転させるものとする。ヘッド機構部（ピックアップ）から特定情報（トラック識別番号やセクタ識別番号やセクタサイズ）を指定することで、対象部分のデータを取得出来るものとする。ここでは、本変形例の説明を分かりやすくするため、ヘッド機構部を通過したデータは、トラックの位置を問わず、全て取得可能であるとする。ここで、被選択コンテンツ位置情報ＳＥＬＰＯＳに含まれる４つの特定情報（ＡＤＤＲ１、ＡＤＤＲ２，ＡＤＤＲ３，ＡＤＤＲ４）のそれぞれに対応するデータ（暗号化部分コンテンツ）が、図７２のように可搬媒体３２（光ディスク）上の位置に記録されているとし、可搬媒体３１（光ディスク）とヘッド機構部も、図７２で示す場所に存在しているとする。

【０２３８】

上記のような状況の場合、実施形態３の動作に沿えば、まず１番目に、特定情報ＡＤＤＲ４に対応するデータ（暗号化部分コンテンツＥＮＣＣＮＴ－４）の読取位置までヘッド機構部が到着するまで可搬媒体３２を回転させてから、該当データを取得する。その後、２番目に特定情報ＡＤＤＲ２に対応するデータ（暗号化部分コンテンツＥＮＣＣＮＴ－２）の読取位置までヘッド機構部が到着するまで可搬媒体３２を回転させ、該当データを取得する。その後も同様に、特定情報ＡＤＤＲ１に対応するデータ（暗号化部分コンテンツＥＮＣＣＮＴ－１）の読取位置までヘッド機構部が到着するまで可搬媒体３２を回転させ、該当データを取得し、最後に、特定情報ＡＤＤＲ３に対応するデータ（暗号化部分コンテンツＥＮＣＣＮＴ－３）の読取位置までヘッド機構部が到着するまで可搬媒体３２を回転させ、該当データを取得する。つまり、特定情報ＡＤＤＲ４に対応するデータを取得するまでに、約１／４周かかり、続いて特定情報ＡＤＤＲ２に対応するデータを取得するまでに、約３／４周かかる。その後も、特定情報ＡＤＤＲ１に対応するデータを取得するまでに、約３／４周かかり、再度に特定情報ＡＤＤＲ３に対応するデータを取得するまでに、約３／４周かかる。つまり、４つのデータ（暗号化部分コンテンツＥＮＣＣＮＴ－４、暗号化部分コンテンツＥＮＣＣＮＴ－２、暗号化部分コンテンツＥＮＣＣＮＴ－１、暗号化部分コンテンツＥＮＣＣＮＴ－３）を取得するまでに、約２．５周必要となることが分かる。

【０２３９】

そこで、本変形例では、上記全４つのデータの取得時間を短くする目的で、部分復号化部３２７は、まずはじめに、それぞれのデータ（暗号化部分コンテンツＥＮＣＣＮＴ－４、暗号化部分コンテンツＥＮＣＣＮＴ－２、暗号化部分コンテンツＥＮＣＣＮＴ－１、暗号化部分コンテンツＥＮＣＣＮＴ－３）を取得する順序の最適値を計算する。このデータを取得する順序の最適値の計算手段を、以後、アクセス順序変更手段と呼ぶ。ここでは、その一例を、図７３を用いて示す。なお、ここでも、４つの特定情報のそれぞれに対応する暗号化部分コンテンツが、図７２のように可搬媒体３２（光ディスク）上の位置に記録されているとし、可搬媒体３１（光ディスク）及びヘッド機構部（ピックアップ）が図７２で示す場所に存在しているとする。

【０２４０】

まず初めに、被選択コンテンツ位置情報ＳＥＬＰＯＳの中の特定情報識別子と特定情報の組を全て取得する。そして、その中から、一番短い時間で取得可能なデータに対する特定情報を取得する。これは、例えば、光ディスク上の物理的な距離（トラック識別番号／セクタ識別番号等を用いて計算可能）などを用いることにより取得出来る。図７２のような状態の場合、一番短い時間で取得可能なデータに対する特定情報は、特定情報ＡＤＤＲ２である。そして、特定情報ＡＤＤＲ２と対応する特定情報識別子ＡＤＤＲ２を、１番初めに取得出来ることを表す順序情報ＮＵＭ１と対応付ける。続いて、次に短い時間（二番目）で取得可能なデータの特定情報を計算する。図７２のような状態の場合、特定情報ＡＤＤＲ４である。そして、同様に、特定情報ＡＤＤＲ４と対応する特定情報識別子ＡＤＤＲ４を、２番目に取得することを表す順序情報ＮＵＭ２と対応付ける。以後同様にして、三番目に短い時間で取得可能なデータの特定情報（特定情報ＡＤＤＲ３）を計算し、特定情報ＡＤＤＲ３と対応する特定情報識別子ＡＤＤＲ３を、３番目に取得することを表す順序情報ＮＵＭ３と対応付け、最後に、四番目に短い時間で取得可能なデータの特定情報（特定情報ＡＤＤＲ１）を計算し、特定情報ＡＤＤＲ１と対応する特定情報識別子ＡＤＤＲ１を、４番目に取得することを表す順序情報ＮＵＭ４と対応付ける。そして、順序情報と特定情報識別子と特定情報の４つの組からなる高速化被選択コンテンツ位置情報ＦＳＥＬＰＯＳ＝（｛ＮＵＭ１、ＡＤＤＲＩＤ２、ＡＤＤＲ２｝、｛ＮＵＭ２、ＡＤＤＲＩＤ４、ＡＤＤＲ４｝、｛ＮＵＭ３、ＡＤＤＲＩＤ３、ＡＤＤＲ３｝、｛ＮＵＭ４、ＡＤＤＲＩＤ１、ＡＤＤＲ１｝）を生成する。続いて、部分復号化部３２７では、高速化被選択コンテンツ位置情報ＦＳＥＬＰＯＳに含まれる順序情報を基に、その順番に従い、特定情報に対応するデータ（暗号化部分コンテンツ）を取得する。最後に、それぞれの暗号化部分コンテンツの復号化を行う。このようにすることで、可搬媒体３１（光ディスク）上に記録されているとびとびの部分データをランダムに取得する（いわゆるランダムアクセス）ような場合にでも、取得したい全てのデータを取得するまでの時間を短縮することが出来る。なお、順序情報ＮＵＭ１、ＮＵＭ２、ＮＵＭ３、ＮＵＭ４の一例は、自然数であり、順序情報ＮＵＭ１に１を、順序情報ＮＵＭ２に２を、順序情報ＮＵＭ３に３を、順序情報ＮＵＭ４に４をそれぞれ割り当ててもよい。さらに、被選択コンテンツ位置情報ＳＥＬＰＯＳには特定情報識別子と特定情報の４組を含んでいたが、当然４組以外であっても良い。

【０２４１】

なお、本変形例で説明したアクセス順序変更手段は、あくまで一例であることを注意しておく。ここでは、他の例を挙げる。以前説明したアクセス順序変更手段の例では、ヘッド機構部を通過したデータは、記録されているトラックの位置を問わず、全て取得可能であると想定していた。しかし、ヘッド機構部（ピックアップ）がいるトラック位置とは異なるトラック位置のデータを取得する場合、可搬媒体３１（光ディスク）が１周回転し、該当読取位置がヘッド機構部を通過しても、該当データが取得出来ない場合がある。これは、該当読取位置に対応するトラック位置へヘッド機構部（ピックアップ）を移動させる時間がかかるなどが原因である。言い換えると、可搬媒体３１（光ディスク）上における内周のトラックから外周方向への移動、もしくは、外周のトラックから内周方向への移動に大きな処理時間がかかることに起因している。可搬媒体３１（光ディスク）上における内側のトラック上にあるデータを読み込んだ後に、外側のトラック上にあるデータを読み込み、その後、また内側のトラック上にあるデータを読み込む場合がその一例である。つまり、これは、可搬媒体３１（光ディスク）上の物理的な距離が近くても、取得時間が短いとは限らないことを意味する。これを鑑みると、アクセス順序変更手段は、取得部３２１（ヘッド機構部や回転軸等）の動作の特徴に依存することが分かる。例えば、取得部３２１が、読取位置のトラック位置とヘッド機構部（ピックアップ）のトラック位置が異なる場合に、データ取得までの時間が多くかかるという特徴を有している場合にでも、アクセス順序変更手段は、特定情報（トラック識別番号／セクタ識別番号等）などを用いて、（光ディスク上の物理的な距離が短いものとは限らず）取得時間が短いものから順に選択し、最適な取得順序を決定しても良い。例えば、一番初めに一番内側のトラック上にある

データを全て取得して、その次に、一つ外側のトラック上にあるデータを全て取得いく、というようなことを繰り返してもよい。この場合、トラック上に一つもデータがない場合は、そのトラックをスキップして次のトラックに進んでもよい。なお、光ディスクの回転制御方式には、角速度一定方式や線速度一定方式があり、これらの特徴を考慮するようにしても良い。

【０２４２】

さらに、なお、部分復号化部３２７のアクセス順序変更手段において、最適な取得順序を決定しやすくするために、可搬媒体３２に記録されるコンテンツ位置情報ＰＯＳの中に含まれる特定情報に特別な情報を追加しても良い。また、可搬媒体３１は当然光ディスクでなくてもよく、例えばハードディスクなどでも同様のことが実現出来る。最後に、なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２４３】

（２８）実施形態３において、特定情報選択部３２６は、予め実行装置３２に与えられているパラメータｂに従って、ヘッダ情報ＨＥＡＤに含むｃ個の特定情報識別子（ＰＯＳＩＤ１、・・・、ＰＯＳＩＤｃ）の中から、ｂ個の特定情報識別子（ｂは１以上ｃ－１以下の自然数）を選択していたが、これに限るものではない。例えば、配信装置３０は可搬媒体３１に、パラメータｂを記録して、実行装置３２は可搬媒体３１に記録されているパラメータｂに従って、ｂ個の特定情報識別子を選択するようにしてもよい。このパラメータｂは、多くすればセキュリティは向上するが、処理時間が多くなり、少なくすれば処理時間は少なくなるが、セキュリティは低下するという特徴を有する。つまり、本変形例を用いることで、コンテンツ配布者のポリシーに依存して、セキュリティレベルなどを設定することが出来るようになる。なお、実行装置３２には、可搬媒体３１にパラメータｂが記録されていない場合、予め与えられるデフォルトのパラメータｂを用いるようにしても良い。なお、実施の形態４においても、同様のことが実現出来る。

【０２４４】

（２９）実施形態３において、可搬媒体３１には、さらに、不正なコンテンツかどうか検証するための情報を持たないコンテンツも同時に記録するようにしても良い。例えば、そのコンテンツの例としては、著作権保護等のセキュリティ技術の比較的必要のない映画のオープニング画面やＤＶＤのメニュー画面などである。そして、実施形態３で説明した実行装置３２による検証処理が終わるまで、それらコンテンツ（オープニング画面やメニュー画面など）を実行するようにしても良い。なお、実施の形態１及び実施の形態２及び実施の形態４においても、同様のことが実現出来る。

【０２４５】

（３０）実施の形態４において、部分コンテンツの属性値（ハッシュ値）を第一ハッシュ値として、一以上の第一ハッシュ値に対する属性値（ハッシュ値）を第二ハッシュ値として、一以上の第二ハッシュ値に対する属性値（ハッシュ値）を一つの結合ハッシュ値として、認証情報ＡＵＴＨはその結合ハッシュ値に対する認証情報としていた（図４３参照）が、これに限るものではない。例えば、図７４に示すように、部分コンテンツの属性値（ハッシュ値）を第一ハッシュ値として、一以上の第一ハッシュ値に対する属性値（ハッシュ値）を第二ハッシュ値として、一以上の第二ハッシュ値に対する属性値（ハッシュ値）を第三ハッシュ値として、一以上の第三ハッシュ値の属性値（ハッシュ値）を一つの結合ハッシュ値として、認証情報ＡＵＴＨはその結合ハッシュ値に対する認証情報としてもよい。この場合、ヘッダ情報ＨＥＡＤには、第一ハッシュ値及び第二ハッシュ値及び第三ハッシュ値を含めることになる。このようにすることによって、可搬媒体から取得しなくてはならないハッシュ値の数を少なくすることが出来、処理時間をさらに短くすることが出来る。

【０２４６】

（３１）実施の形態１の可搬媒体１１において記録されているデータに加え、さらに、可搬媒体に部分コンテンツの実行手順を記述したデータである実行手順データＮＡＶを記

録していており、実行装置１２の実行部１２９では、その実行手順データＮＡＶを基に、部分コンテンツを実行するような場合に、可搬媒体に、さらに、図７５で示すように、その実行手順データＮＡＶに対する認証情報として実行手順データ認証情報ＮＡＶＡＵＴＨを記録するようにして、認証情報検証部１２６では、その実行手順データ認証情報ＮＡＶＡＵＴＨが実行手順データＮＡＶに対する正規の認証情報である場合にのみ、実行部１２９へ暗号化コンテンツＥＮＣＣＮＴ及びコンテンツ鍵ＣＫを出力するようにしてもよい。ここで、実行手順データＮＡＶは、例えば、ＤＶＤ－ＶＩＤＥＯ形式におけるナビゲーションファイル（拡張子がＩＦＯのファイル）である。これにより、万が一、コンテンツ位置情報ＰＯＳが攻撃者に漏洩し、その攻撃者が代表部分コンテンツ以外の部分コンテンツと不正部分コンテンツを入れ替え（図７６参照）、実行手順データＮＡＶがその代表部分コンテンツをとばして（スキップして）実行するように書き換えられた場合にも、実行装置１２では、その実行手順データ認証情報ＮＡＶＡＵＴＨを検証することによって、実行手順データＮＡＶが改ざんされたことを検知し、実行部１２９ではその不正部分コンテンツを含んだ不正コンテンツを実行しないようになる。これにより、さらに強い不正コンテンツをも検知できる不正コンテンツ検知システムが実現出来る。なお、実施の形態２及び３及び実施の形態４においても、同様のことが実現出来る。

【０２４７】

（３２）実施の形態４において、実行装置４２の取得部４２１は、可搬媒体４１から暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴを一度に取得していたが、これに限るものではない。例えば、取得部４２１は可搬媒体４１から、初めに暗号化鍵束ＫＢだけを取得し、コンテンツ鍵取得部４２３の処理を行う。そして、コンテンツ鍵取得部４２３での処理が正しく終了した場合にのみ、特定情報選択部４２４は、取得部４２１経由で、可搬媒体４１からコンテンツ位置情報ＰＯＳを取得してから、特定情報選択部４２４の処理を行う。そして、部分復号化部４２５は、取得部４２１経由で、可搬媒体４１から、特定情報選択部４２４で選択された特定情報に対応する暗号化部分コンテンツだけを取得してから、部分復号化部４２５の処理を行う。そして、認証情報検証部４２７は、取得部３２１経由で、ヘッダ情報ＨＥＡＤに中で認証情報検証部４２７の処理に必要な情報のみを取得し、認証情報検証部４２７の処理を行う。そして、認証情報検証部４２７での検証が成功した場合に、実行部４２８は、可搬媒体４１から暗号化コンテンツＥＮＣＣＮＴ（もしくは、部分復号化部４２５で取得された暗号化部分コンテンツ以外の暗号化部分コンテンツ）を逐次取得し、実行部４２８の処理を行うようにしても良い。そうすることにより、可搬媒体４１内の必要のない情報は取得しないようになり、さらに、可搬媒体４１内に不正な認証情報もしくは不正なヘッダ情報が記録されている場合には、実行装置４２は暗号化コンテンツＥＮＣＣＮＴを取得しないようになるため、実行装置の処理負荷が軽減されるという利点が生まれる。なお、実施の形態１及び実施の形態２及び実施の形態３においても、同様のことが実現出来る。

【０２４８】

（３３）実施の形態４において、可搬媒体４２に記録されるヘッダ情報ＨＥＡＤは、見出し情報として、暗号化コンテンツＥＮＣＣＮＴの必ず前側についているとは限らない。例えば、ヘッダ情報ＨＥＡＤではなく、付加情報として、暗号化コンテンツＥＮＣＣＮＴの後ろ側（フッタ）についていても構わない。なお、実施の形態１及び実施の形態２及び実施の形態３においても、同様のことが実現出来る。

【０２４９】

（３４）実施の形態４において、認証情報ＡＵＴＨは、結合ハッシュ値に対するデジタル署名であったが、実行装置４２においてヘッダ情報ＨＥＡＤに含まれるｅ個の第二ハッシュ値を連結した値の正当性を検証出来るものであれば、どのようなものでも良い。例えば、非特許文献１に記載のＤＳＡ方式やＲＳＡ署名は、動作の一部として、ハッシュ関数を用いて署名生成対象メッセージの属性値（ハッシュ値）を生成する処理も含んでいる。このような場合、認証情報ＡＵＴＨは、ｅ個の第二ハッシュ値を結合した値に対する属性

値である結合ハッシュ値に対するデジタル署名ではなく、図７７で示すように、ｅ個の第二ハッシュ値を結合した値ＨＡＳＨ２―１｜｜ＨＡＳＨ２―２｜｜・・・｜｜ＨＡＳＨ２―ｅに対するデジタル署名でも良い。この場合、認証情報検証部４２７は、例えば、図７８のような動作となり、認証情報ＡＵＴＨ（デジタル署名）が、ｅ個の第二ハッシュ値を結合した値に対する正規の認証情報（デジタル署名）であるか検証することになる。また、デジタル署名方式を用いずにＡＥＳなどの秘密鍵暗号を用いても同様のことが実現出来る。まず、認証情報生成情報格納部４００７及び検証情報格納部４２５には、同じ鍵Ｋが与えられているとする。そして、認証情報生成部４００８では、鍵Ｋを用いてヘッダ情報ＨＥＡＤに含まれるｅ個のハッシュ値を連結した値を暗号化した暗号文を認証情報ＡＵＴＨとする。（なお、ここで、一方向性関数を用いて、ｋ個のハッシュ値を連結した値を小さなサイズの値に変換してもよい）。認証情報検証部４２６では、鍵Ｋを用いて入力された認証情報ＡＵＴＨを復号化し、その復号結果がヘッダ情報ＨＥＡＤと一致していては、認証情報ＡＵＴＨは正当であると判断する。このようにして、デジタル署名アルゴリズムを使用しなくても、ヘッダ情報の正当性を検証することが出来る。同様に、一方向性関数や鍵付き一方向性関数などを用いても同様に実現出来る。なお、実施の形態３においても、同様にデジタル署名アルゴリズムの替わりに、ＡＥＳなどの秘密鍵暗号や一方向性関数や鍵付き一方向性関数などを利用出来る。

【０２５０】

（３５）実施の形態２において、コンテンツＣＮＴを構成するｃ個の部分コンテンツからｋ×ｍ個の代表部分コンテンツを選択していたが、ここでｃ個の部分コンテンツが全て代表部分コンテンツとして選択されるようにしてもよい。また、同じ一つの部分コンテンツが異なる代表部分コンテンツとして選択されるようにしてもよい。このようにすることによって、コンテンツの中のどの一部分（部分コンテンツ）を、不正なコンテンツに差し替えられても、ある確率でコンテンツの実行、再生を停止することが出来るようになり、安全性が向上する。なお、実施の形態１においても同様のことが実現出来る。

【０２５１】

（３６）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、ＣＤ、ＭＯ、ＤＶＤ、ＳＤメモリカード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０２５２】

（３７）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０２５３】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人・団体・会社）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御（例えば警告、停止、禁止）することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般

、特に記録媒体や可搬媒体（例えば光ディスクやメモリカード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【０２５４】

さらに、本発明は、動画データや音声データなどのマルチメディアコンテンツに限らず、コンテンツの実行順序を制御する実行順序ファイル（ナビゲーションファイル）や、コンピュータプログラム等の保護にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しない等が実現出来る。そのため、安全（セキュア）な処理環境を実現するコンピュータシステム全般、特にＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）等としても有用である。

【図面の簡単な説明】

【０２５５】

【図１】本発明の実施の形態１における不正コンテンツ検知システムの概要図

【図２】本発明の実施の形態１における配布センタ１０の構成例を示す図

【図３】本発明の実施の形態１におけるコンテンツＣＮＴの一例を示す図

【図４】本発明の実施の形態１における実行装置情報格納部１００３の構成例を示す図

【図５】本発明の実施の形態１における暗号化鍵束ＫＢの一例を示す図

【図６】本発明の実施の形態１における代表部分コンテンツと特定情報の一例を示す図

【図７】本発明の実施の形態１におけるコンテンツ位置情報ＰＯＳの一例を示す図

【図８】本発明の実施の形態１におけるヘッダ情報ＨＥＡＤの一例を示す図

【図９】本発明の実施の形態１における暗号化コンテンツＥＮＣＣＮＴの一例を示す図

【図１０】本発明の実施の形態１における配布センタ１０の処理の流れ図（一例）

【図１１】本発明の実施の形態１における可搬媒体１１に記録されるデータの一例

【図１２】本発明の実施の形態１における実行装置１２の構成例を示す図

【図１３】本発明の実施の形態１における実行装置１２の処理の流れ図（一例）

【図１４】本発明の実施の形態２における不正コンテンツ検知システムの概要図

【図１５】本発明の実施の形態２における配布センタ２０の構成例を示す図

【図１６】本発明の実施の形態２における配布センタ２０の処理の流れ図（一例）

【図１７】本発明の実施の形態２における可搬媒体２１に記録されるデータの一例

【図１８】本発明の実施の形態２における実行装置２２の構成例を示す図

【図１９】本発明の実施の形態２における実行装置２２の処理の流れ図（一例）

【図２０】本発明の実施の形態３における不正コンテンツ検知システムの概要図

【図２１】本発明の実施の形態３における配布センタ３０の構成例を示す図

【図２２】本発明の実施の形態３における実行装置情報格納部３００３の構成例を示す図

【図２３】本発明の実施の形態３における暗号化鍵束ＫＢの一例を示す図

【図２４】本発明の実施の形態３におけるコンテンツＣＮＴの一例を示す図

【図２５】本発明の実施の形態３におけるコンテンツ位置情報ＰＯＳの一例を示す図

【図２６】本発明の実施の形態３におけるヘッダ情報ＨＥＡＤの一例を示す図

【図２７】本発明の実施の形態３における認証情報ＡＵＴＨの作成方法の一例を示す図

【図２８】本発明の実施の形態３における暗号化コンテンツＥＮＣＣＮＴの一例を示す図

【図２９】本発明の実施の形態３における配布センタ３０の処理の流れ図（一例）

【図３０】本発明の実施の形態３における可搬媒体３１に記録されるデータの一例

【図３１】本発明の実施の形態３における実行装置３２の構成例を示す図

【図３２】認証情報検証部３２５、及び、ヘッダ情報検証部３２８の動作の一例を示

す図
【図３３】本発明の実施の形態３における被選択ヘッダ情報ＳＥＬＨＥＡＤの一例を示す図
【図３４】本発明の実施の形態３における被選択コンテンツ位置情報ＳＥＬＰＯＳの一例を示す図
【図３５】本発明の実施の形態３における暗号化コンテンツＥＮＣＣＮＴの一例を示す図
【図３６】本発明の実施の形態３における実行装置３２の処理の流れ図（一例）
【図３７】本発明の実施の形態４における不正コンテンツ検知システムの概要図
【図３８】本発明の実施の形態４における配布センタ４０の構成例を示す図
【図３９】本発明の実施の形態４における実行装置情報格納部４００３の構成例を示す図
【図４０】本発明の実施の形態４における暗号化鍵束ＫＢの一例を示す図
【図４１】本発明の実施の形態４におけるコンテンツＣＮＴの一例を示す図
【図４２】本発明の実施の形態４におけるコンテンツ位置情報ＰＯＳの一例を示す図
【図４３】本発明の実施の形態４における認証情報ＡＵＴＨの作成方法の一例を示す図
【図４４】本発明の実施の形態４におけるヘッダ情報ＨＥＡＤの一例を示す図
【図４５】本発明の実施の形態４における暗号化コンテンツＥＮＣＣＮＴの一例を示す図
【図４６】本発明の実施の形態４における配布センタ４０の処理の流れ図（一例）
【図４７】本発明の実施の形態４における可搬媒体４１に記録されるデータの一例
【図４８】本発明の実施の形態４における実行装置４２の構成例を示す図
【図４９】本発明の実施の形態４における被選択コンテンツ位置情報ＳＥＬＰＯＳの一例を示す図
【図５０】本発明の実施の形態３における暗号化コンテンツＥＮＣＣＮＴの一例を示す図
【図５１】認証情報検証部４２７の動作の一例を示す図
【図５２】本発明の実施の形態４における実行装置４２の処理の流れ図（一例）
【図５３】可搬媒体１１に記録されるデータの別の一例
【図５４】可搬媒体１１に記録されるコンテンツ認証情報ＣＮＴＡＵＴＨの一例
【図５５】可搬媒体１１に記録されるデータの別の一例
【図５６】可搬媒体１１に記録されるコンテンツ認証情報ＣＮＴＡＵＴＨの別の一例
【図５７】可搬媒体１１に記録されるデータの別の一例
【図５８】可搬媒体１１に記録されるデータの別の一例
【図５９】認証情報ＡＵＴＨを作成するヘッダ情報ＨＥＡＤの別の一例
【図６０】ヘッダ情報ＨＥＡＤの別の一例
【図６１】認証情報生成情報格納部１００７の別の一例
【図６２】検証情報格納部１２５の別の一例
【図６３】認証情報生成情報格納部１００７の別の一例
【図６４】検証情報格納部１２５の別の一例
【図６５】本発明の実施の形態３における可搬媒体３１に記録されるデータの別の一例
【図６６】本発明の実施の形態３における可搬媒体３１に記録されるデータの別の一例
【図６７】本発明の実施の形態３における第二ヘッダ情報ＨＥＡＤｘの一例
【図６８】本発明の実施の形態３における配布センタ３０の構成例を示す別の図
【図６９】本発明の実施の形態３における可搬媒体３１に記録されるデータの別の一例
【図７０】本発明の実施の形態３における可搬媒体３１に記録されるデータの別の一

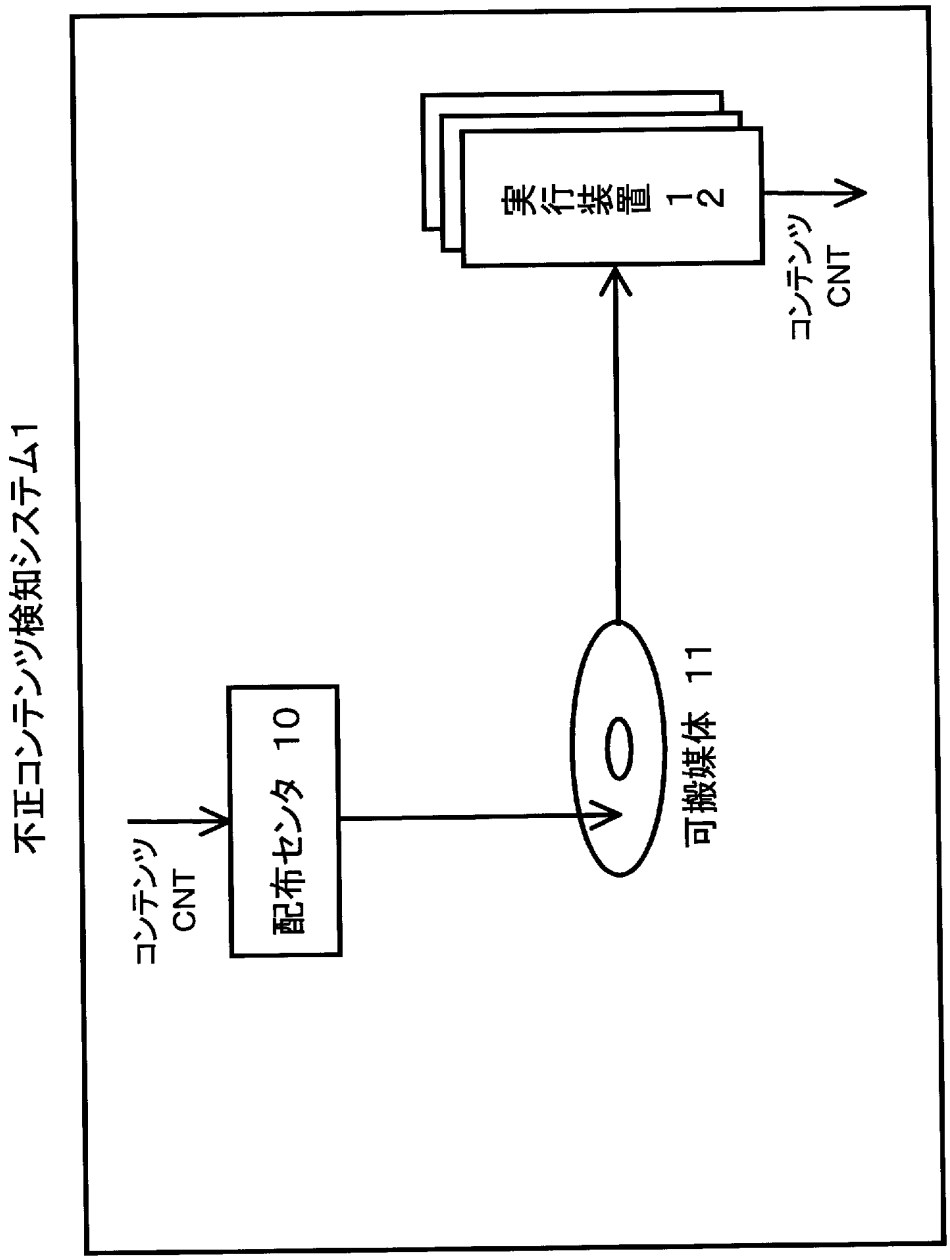
例
【図７１】本発明の実施の形態３における、被選択コンテンツ位置情報ＳＥＬＰＯＳの別の一例
【図７２】本発明の実施の形態３における、可搬媒体３２（光ディスク）と取得部３２１の一例
【図７３】本発明の実施の形態３における、被選択コンテンツ位置情報ＳＥＬＰＯＳとアクセス順序変更手段と高速化被選択コンテンツ位置情報ＦＳＥＬＰＯＳの一例
【図７４】本発明の実施の形態４における、認証情報ＡＵＴＨの作成方法の別の一例
【図７５】本発明の実施の形態１の可搬媒体１１に記録されるデータの別の一例
【図７６】本発明の実施の形態１において、代表部分コンテンツ以外の部分コンテンツと不正部分コンテンツを入れ替えた場合の不正コンテンツの一例
【図７７】本発明の実施の形態４における、認証情報ＡＵＴＨの作成方法の別の一例
【図７８】本発明の実施の形態４における、認証情報検証部４２７の別の動作例
【図７９】従来技術の可搬媒体に記録されるデータ

【符号の説明】

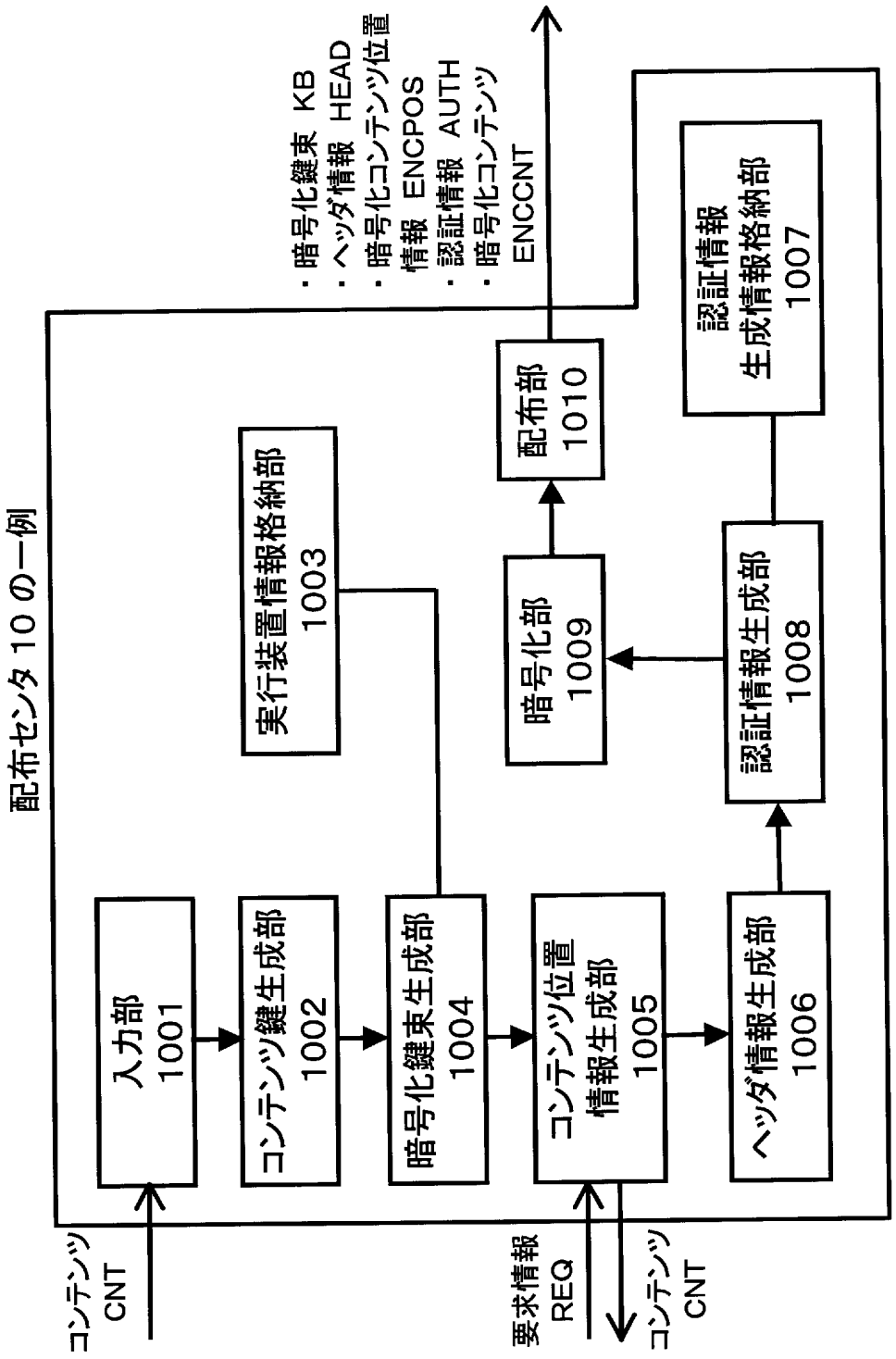
【０２５６】

１０、２０、３０、４０　配布センタ
１１、２１、３１、４１　可搬媒体
１２、２２、３２、４２　実行装置
１００１、３００１、４００１　入力部
１００２、３００２，４００２　コンテンツ鍵生成部
１００３、３００３，４００３　実行装置情報格納部
１００４、３００４，４００４　暗号化鍵束生成部
１００５、２００５、３００５、４００５　コンテンツ位置情報生成部
１００６、２００６、３００６、４００６　ヘッダ情報生成部
１００７、３００７、４００７　認証情報生成情報格納部
１００８、２００８、３００８、４００８　認証情報生成部
１００９、２００９、３００９、４００９　暗号化部
１０１０、２０１０、３０１０、４０１０　配布部
１２１、２２１、３２１、４２１　取得部
１２２、３２２、４２２　デバイス鍵格納部
１２３、３２３、４２３　コンテンツ鍵取得部
１２４　コンテンツ位置情報取得部
３２６、４２４　特定情報選択部
１２５、３２４、４２６　検証情報格納部
１２６、３２５、４２７　認証情報検証部
１２７、３２７、４２５　部分復号化部
１２８、３２８　ヘッダ情報検証部
１２９、３２９、４２８　実行部

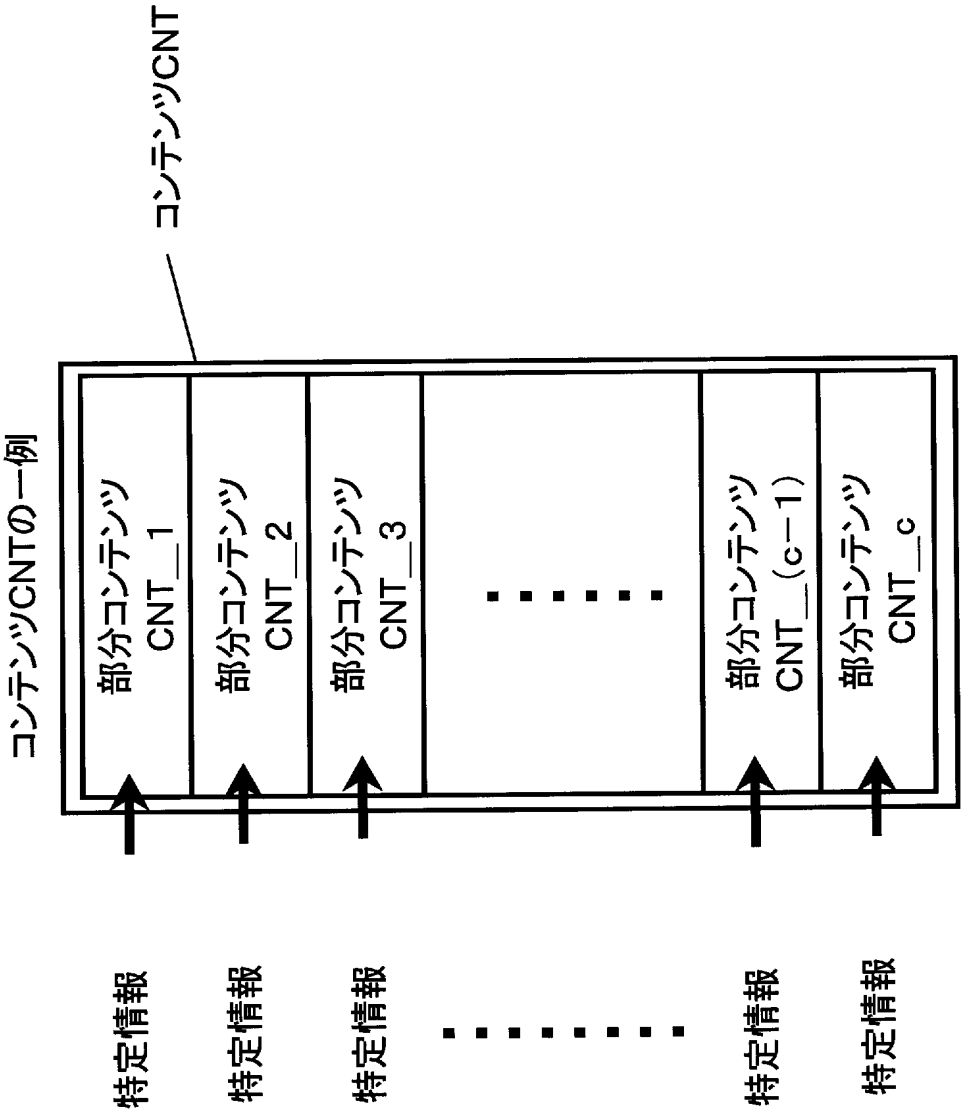
【書類名】図面
【図１】



【図２】

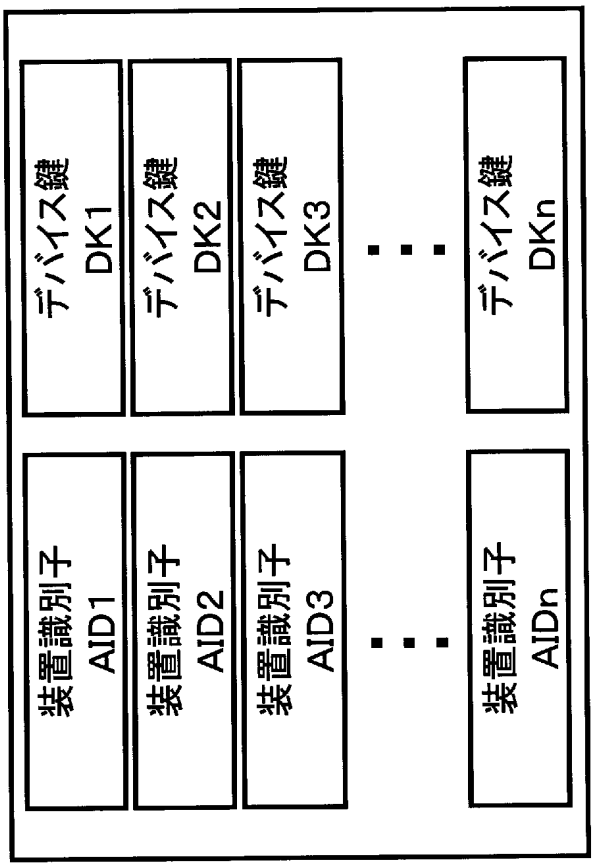

配布センタ10の一例
コンテンツ CNT
入力部 1001
コンテンツ鍵生成部 1002
暗号化鍵束生成部 1004
コンテンツ位置情報生成部 1005
ヘッダ情報生成部 1006
実行装置情報格納部 1003
暗号化部 1009
配布部 1010
認証情報生成部 1008
認証情報生成格納部 1007
要求情報 REQ
コンテンツ CNT
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・暗号化コンテンツ位置情報 ENCPOS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

【図３】

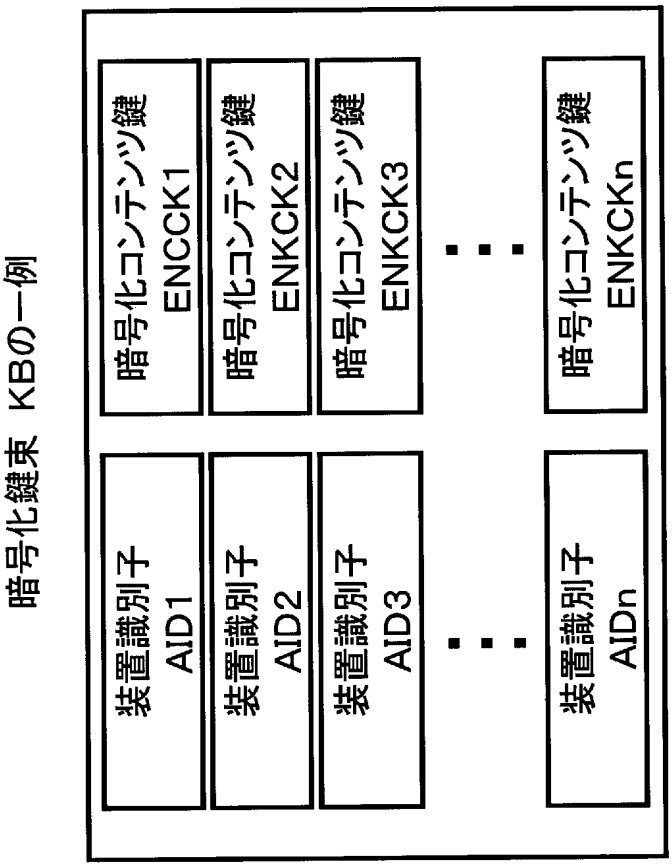

コンテンツCNTの一例
コンテンツCNT
部分コンテンツ CNT_1
部分コンテンツ CNT_2
部分コンテンツ CNT_3
部分コンテンツ CNT_(c−1)
部分コンテンツ CNT_c
特定情報
特定情報
特定情報
特定情報
特定情報

【図４】

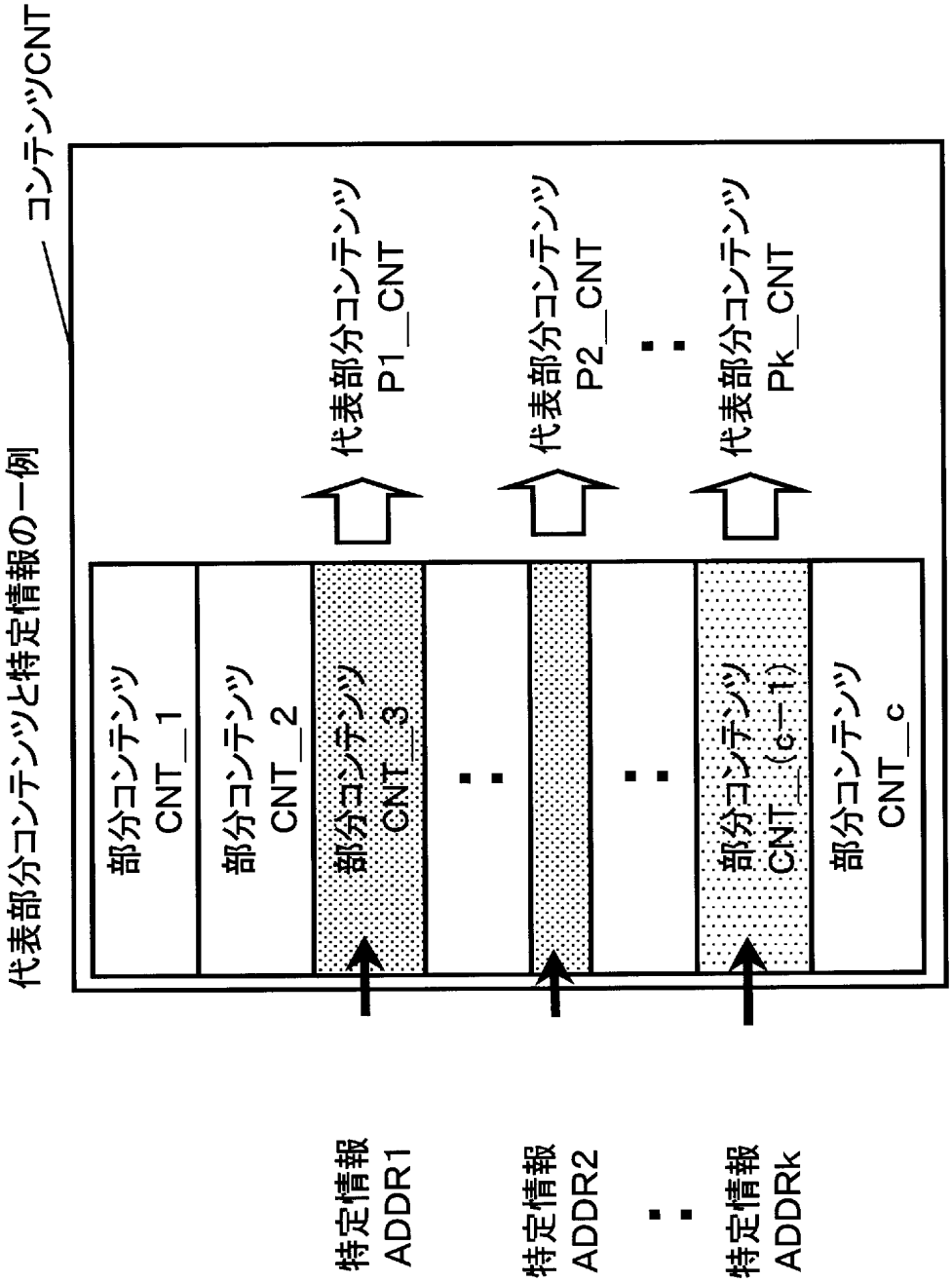
実行装置情報格納部1003の一例



【図５】

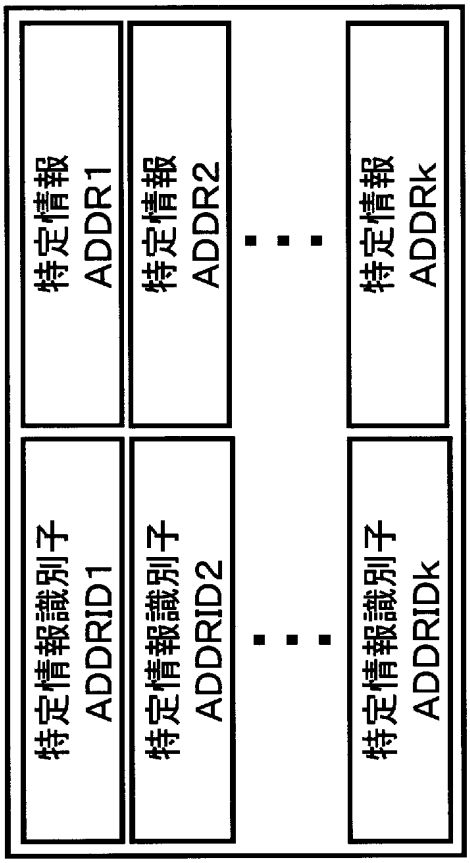

暗号化鍵束　KBの一例
装置識別子
AID1
装置識別子
AID2
装置識別子
AID3
装置識別子
AIDn
暗号化コンテンツ鍵
ENCCK1
暗号化コンテンツ鍵
ENKCK2
暗号化コンテンツ鍵
ENKCK3
暗号化コンテンツ鍵
ENKCKn

【図６】


代表部分コンテンツと特定情報の一例
コンテンツCNT
部分コンテンツ CNT_1
部分コンテンツ CNT_2
部分コンテンツ CNT_3
部分コンテンツ CNT_(c−1)
部分コンテンツ CNT_c
代表部分コンテンツ P1_CNT
代表部分コンテンツ P2_CNT
代表部分コンテンツ Pk_CNT
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDRk

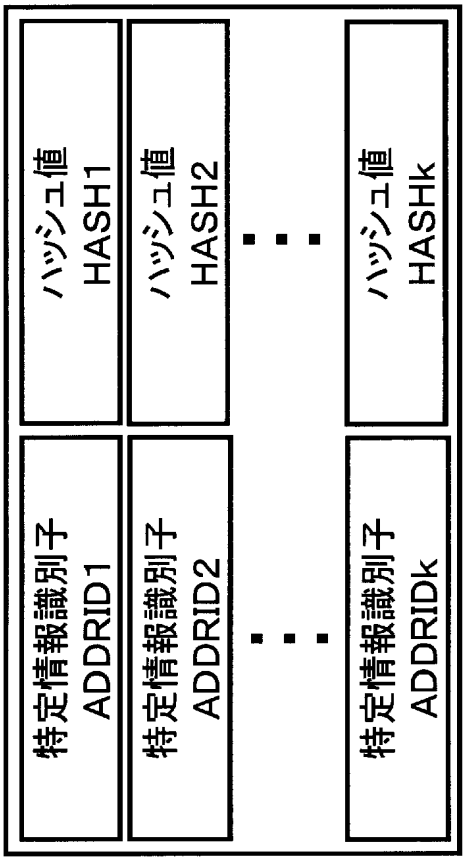
【図７】

コンテンツ位置情報　POSの一例

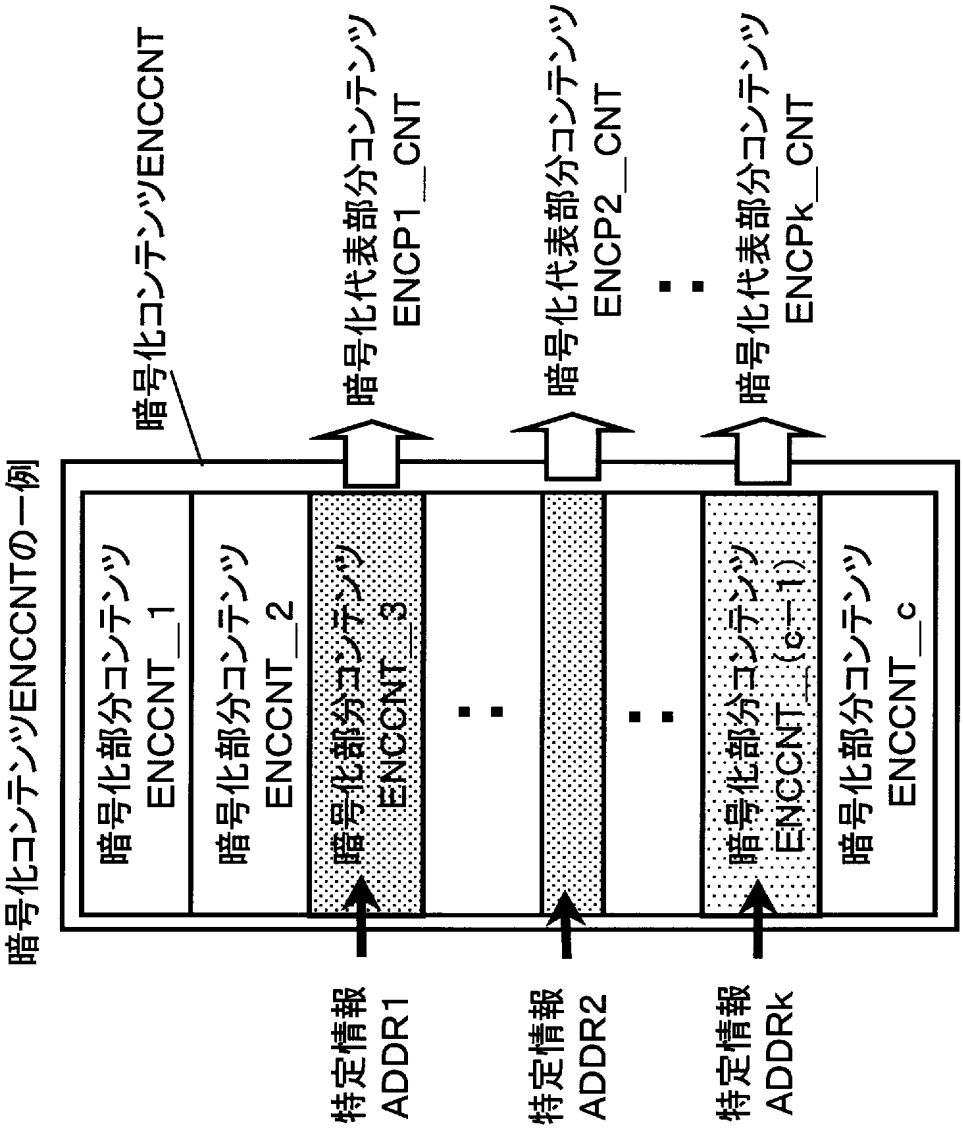


【図８】

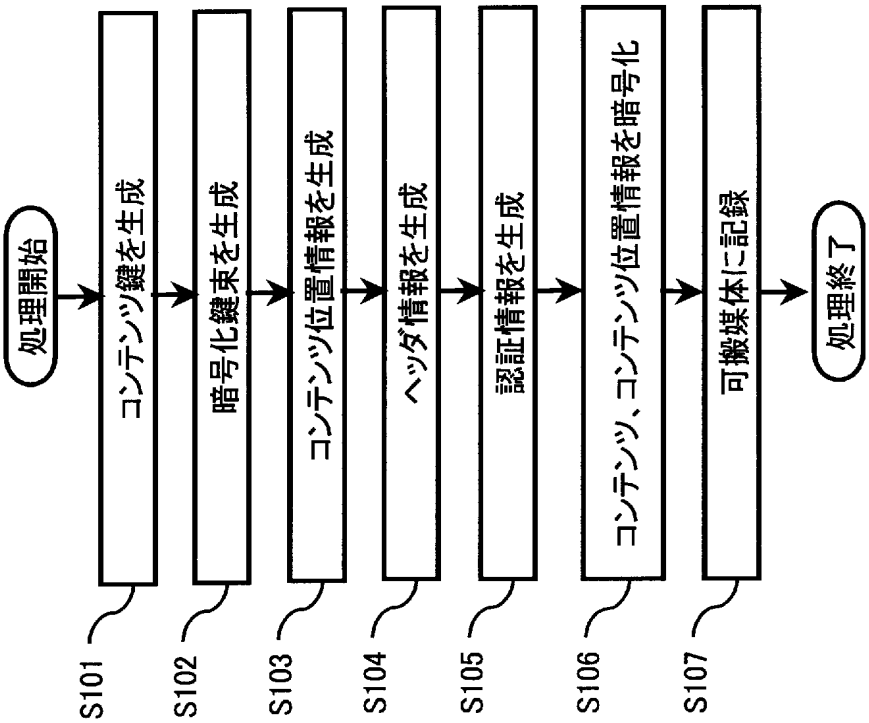
ヘッダ情報　HEADの一例



【図９】

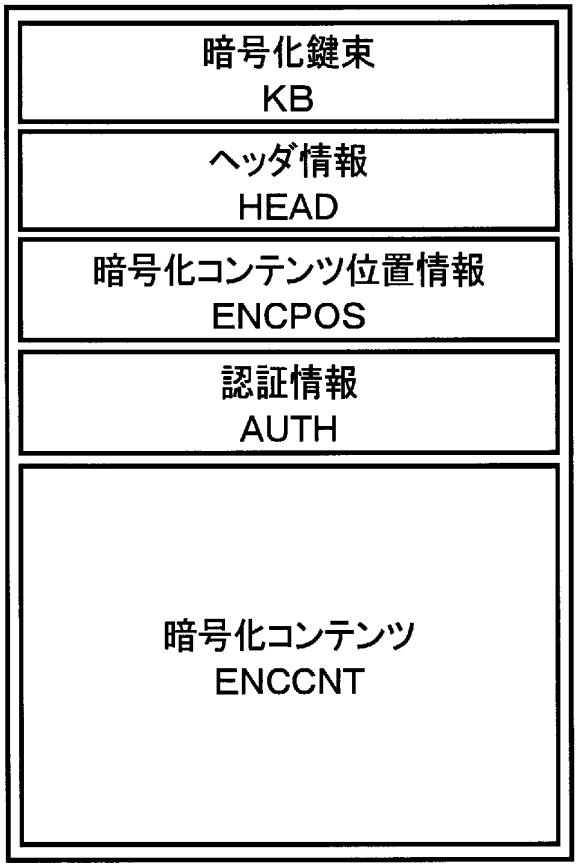

暗号化コンテンツENCCNTの一例
暗号化コンテンツENCCNT
暗号化部分コンテンツ ENCCNT_1
暗号化部分コンテンツ ENCCNT_2
暗号化部分コンテンツ ENCCNT_3
暗号化部分コンテンツ ENCCNT_(c－1)
暗号化部分コンテンツ ENCCNT_c
暗号化代表部分コンテンツ ENCP1_CNT
暗号化代表部分コンテンツ ENCP2_CNT
暗号化代表部分コンテンツ ENCPk_CNT
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDRk

【図１０】

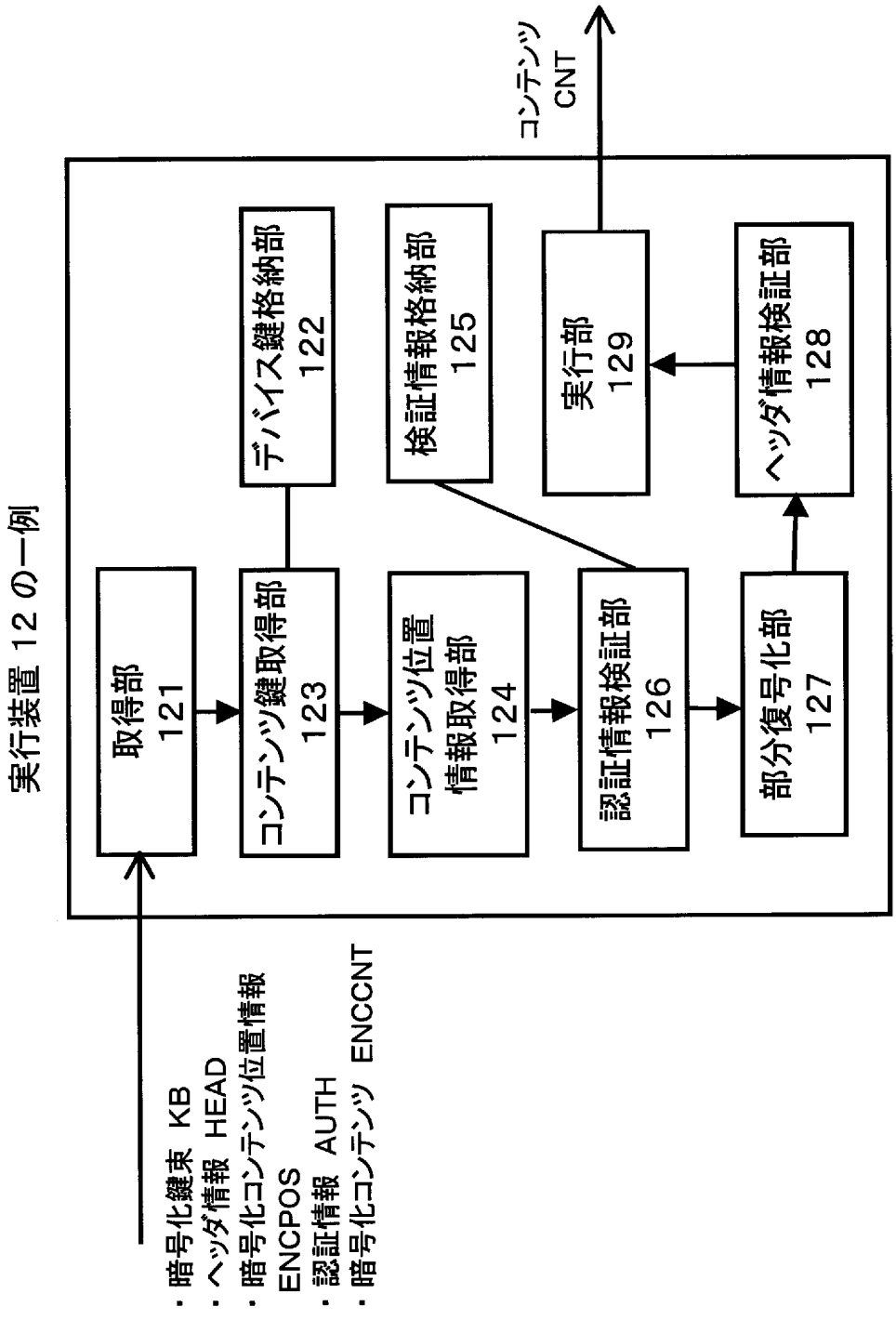

処理開始
コンテンツ鍵を生成
暗号化鍵束を生成
コンテンツ位置情報を生成
ヘッダ情報を生成
認証情報を生成
コンテンツ、コンテンツ位置情報を暗号化
可搬媒体に記録
処理終了
S101
S102
S103
S104
S105
S106
S107

【図１１】

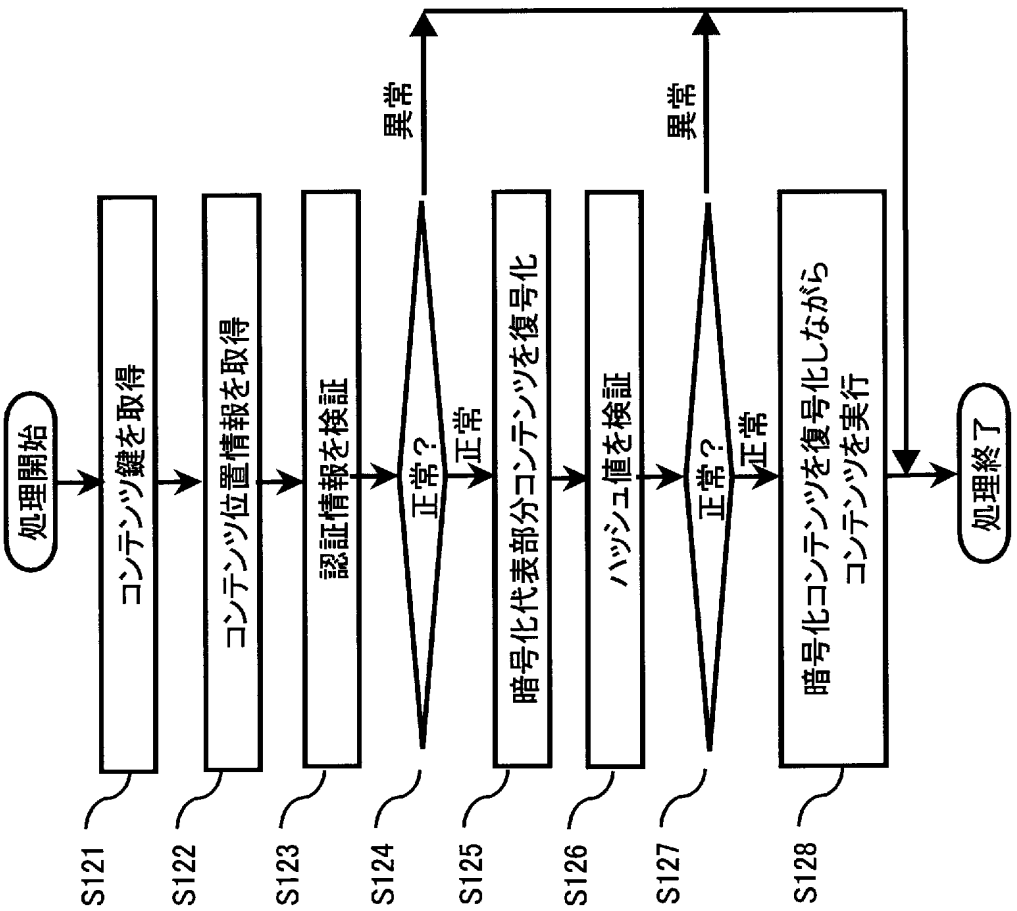
可搬媒体11に記録されるデータの一例



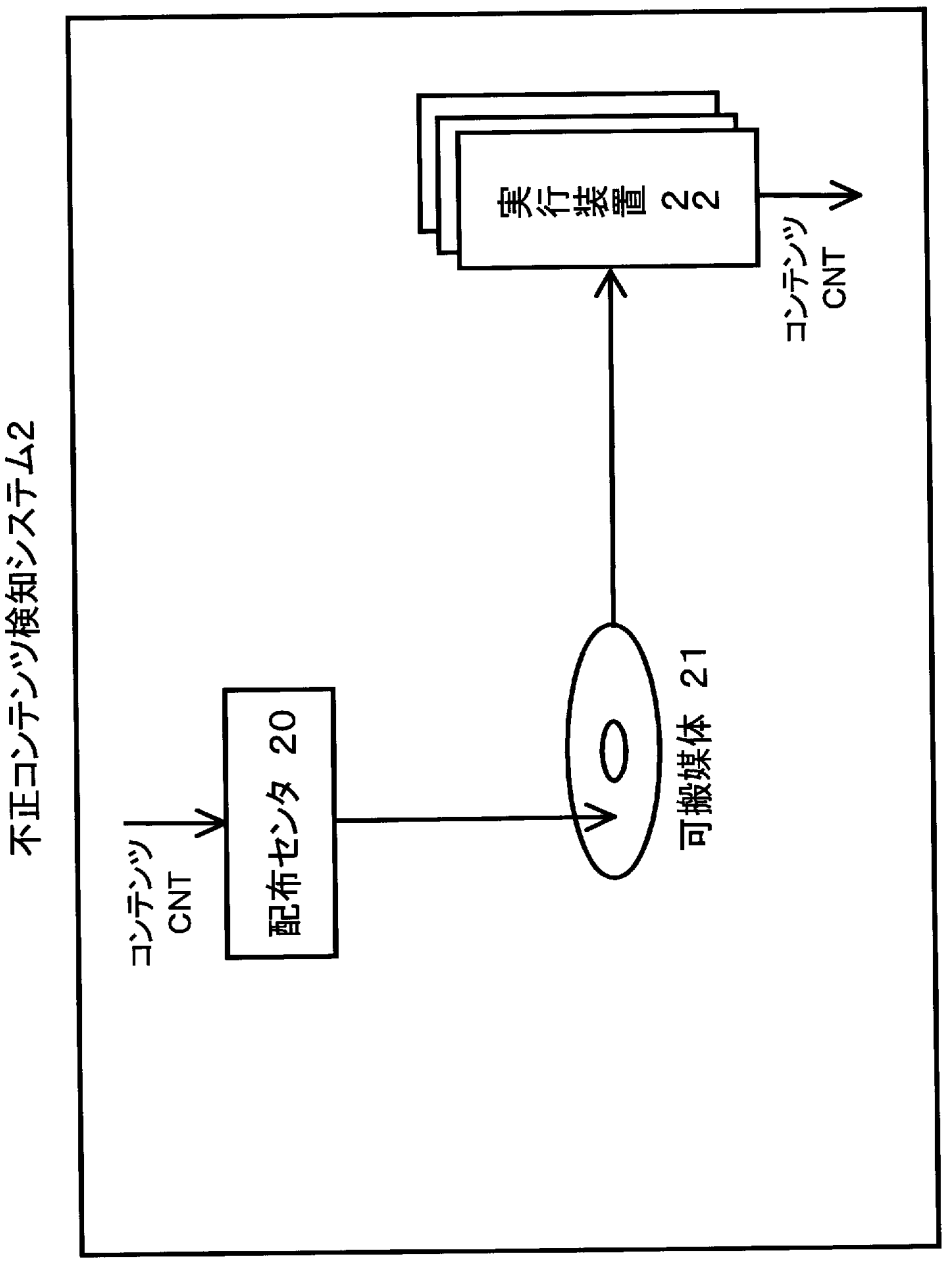
【図１２】


実行装置 12 の一例
取得部 121
コンテンツ鍵取得部 123
デバイス鍵格納部 122
コンテンツ位置情報取得部 124
検証情報格納部 125
認証情報検証部 126
部分復号化部 127
ヘッダ情報検証部 128
実行部 129
コンテンツ CNT
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・暗号化コンテンツ位置情報 ENCPOS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

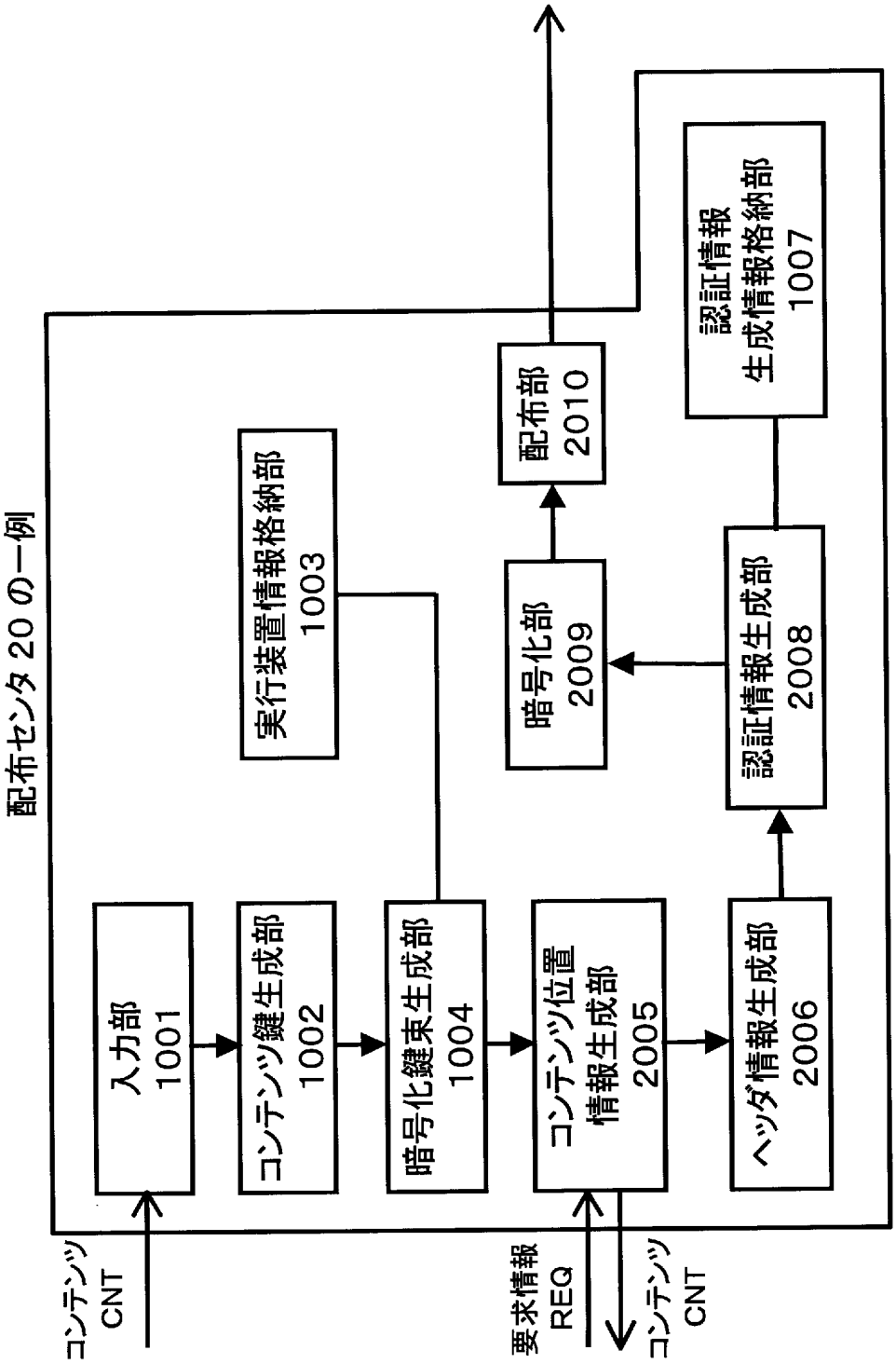
【図１３】


処理開始
コンテンツ鍵を取得
コンテンツ位置情報を取得
認証情報を検証
正常？
異常
正常
暗号化代表部分コンテンツを復号化
ハッシュ値を検証
正常？
異常
正常
暗号化コンテンツを復号化しながら
コンテンツを実行
処理終了
S121
S122
S123
S124
S125
S126
S127
S128

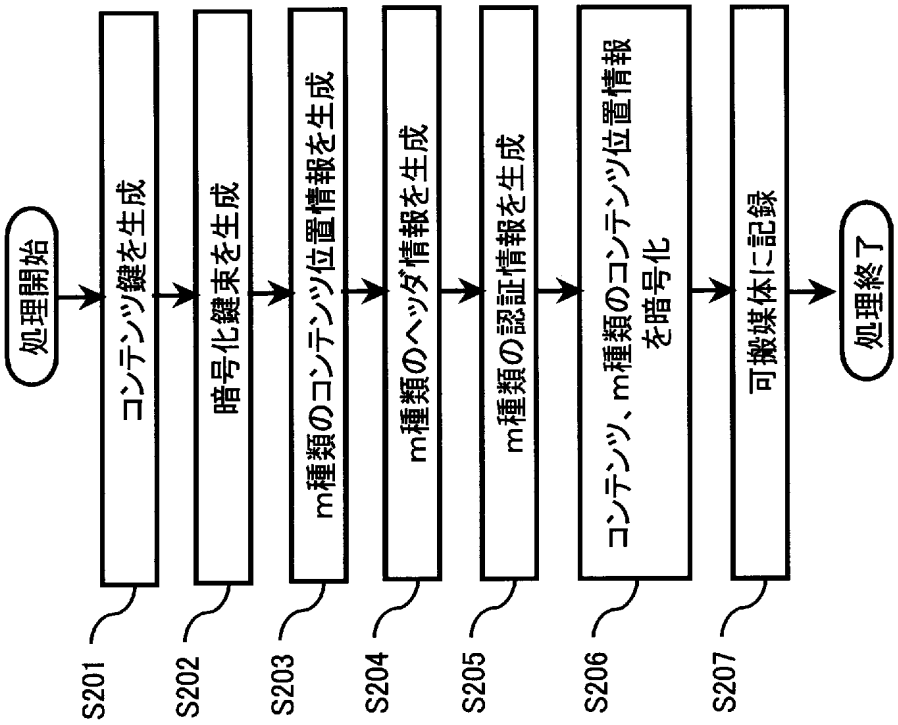
【図１４】



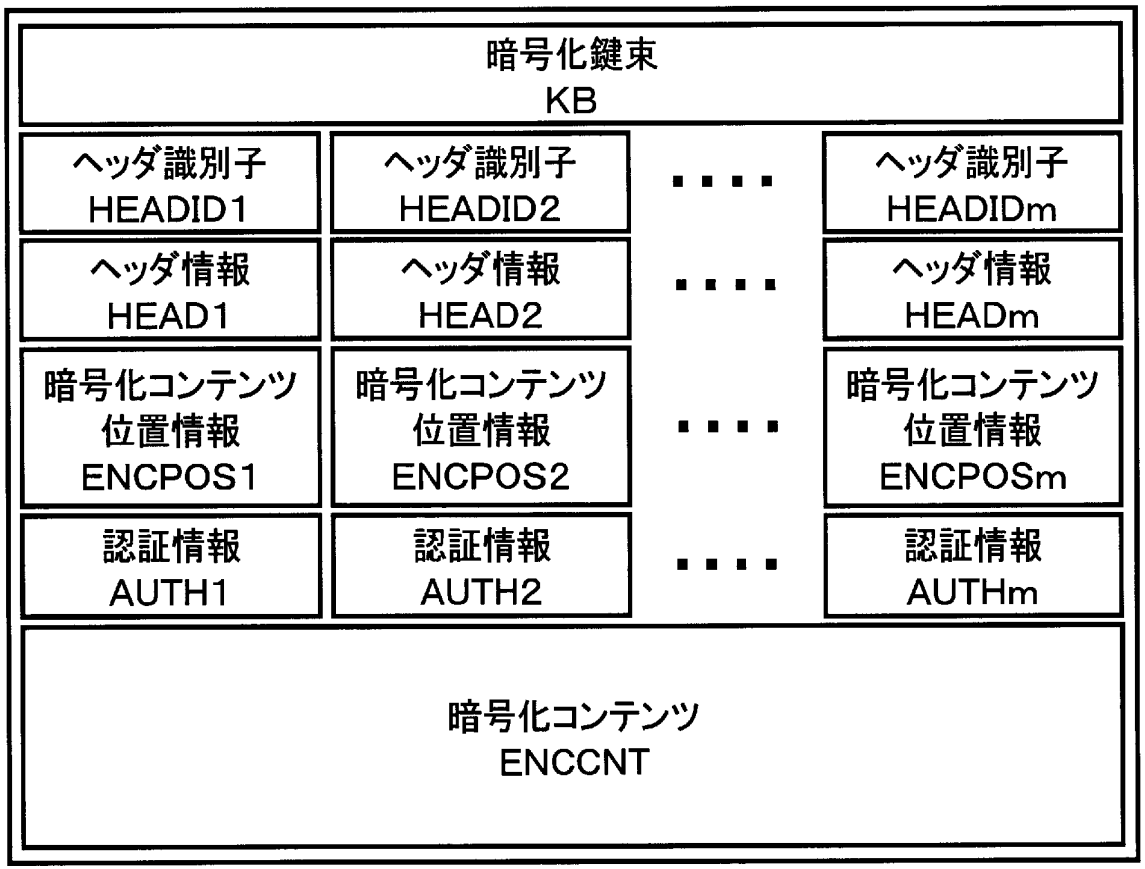
【図１５】


配布センタ20の一例
入力部
1001
コンテンツ鍵生成部
1002
暗号化鍵束生成部
1004
コンテンツ位置
情報生成部
2005
ヘッダ情報生成部
2006
実行装置情報格納部
1003
暗号化部
2009
配布部
2010
認証情報生成部
2008
認証情報
生成情報格納部
1007
コンテンツ
CNT
要求情報
REQ
コンテンツ
CNT

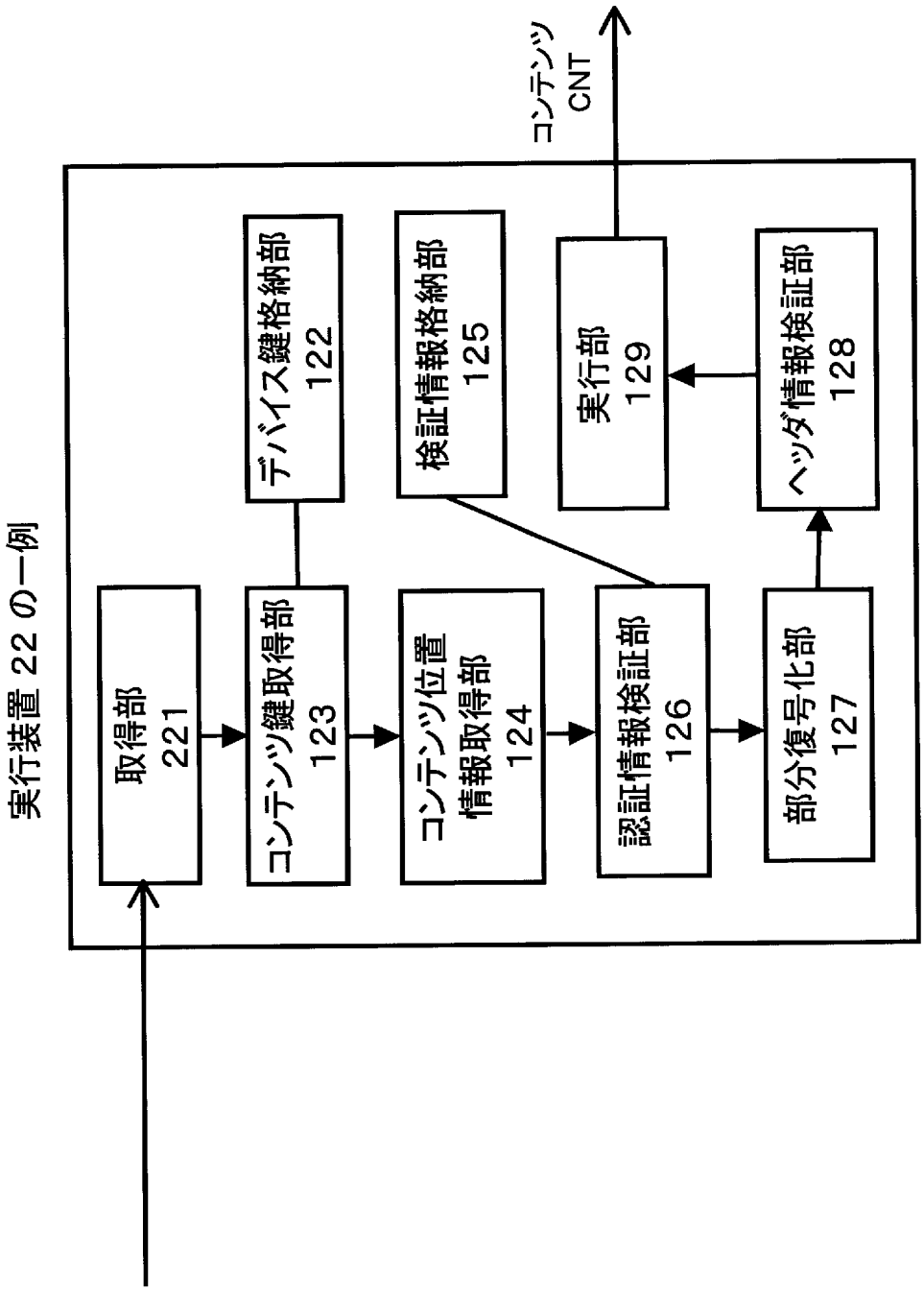
【図１６】


処理開始
コンテンツ鍵を生成
暗号化鍵束を生成
m種類のコンテンツ位置情報を生成
m種類のヘッダ情報を生成
m種類の認証情報を生成
コンテンツ、m種類のコンテンツ位置情報を暗号化
可搬媒体に記録
処理終了
S201
S202
S203
S204
S205
S206
S207

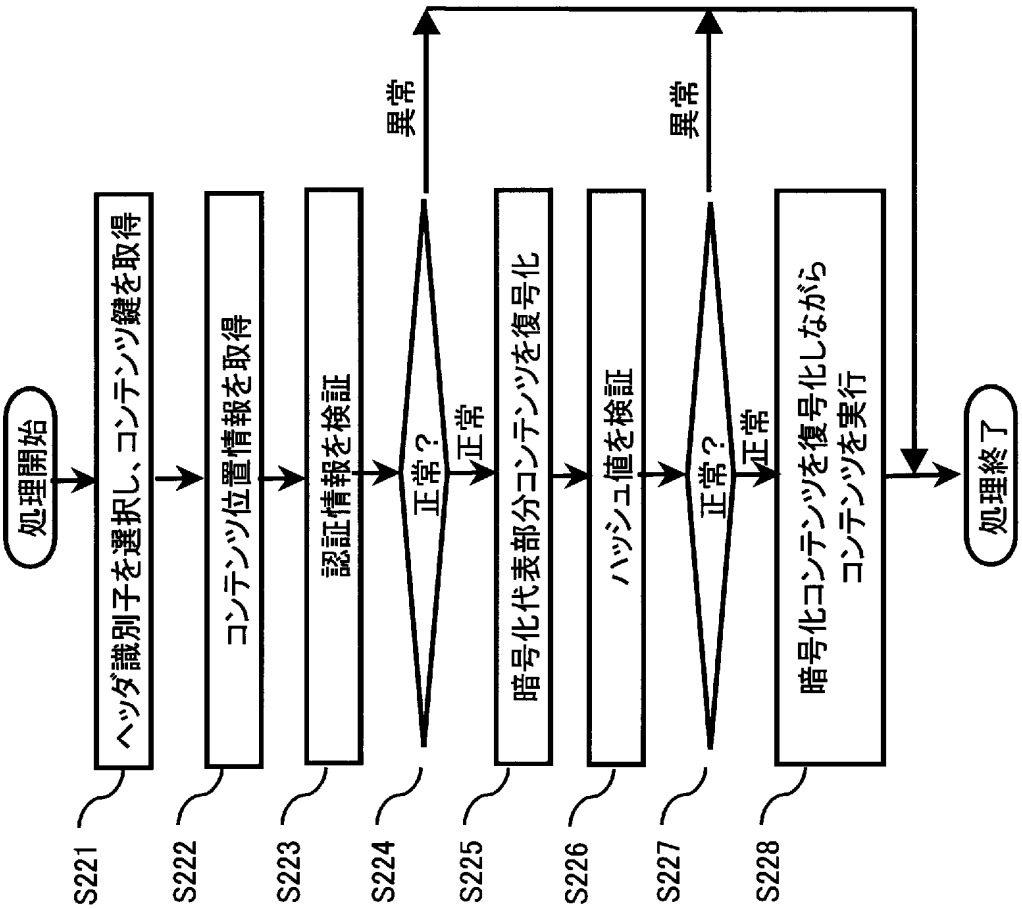
可搬媒体21に記録されるデータの一例



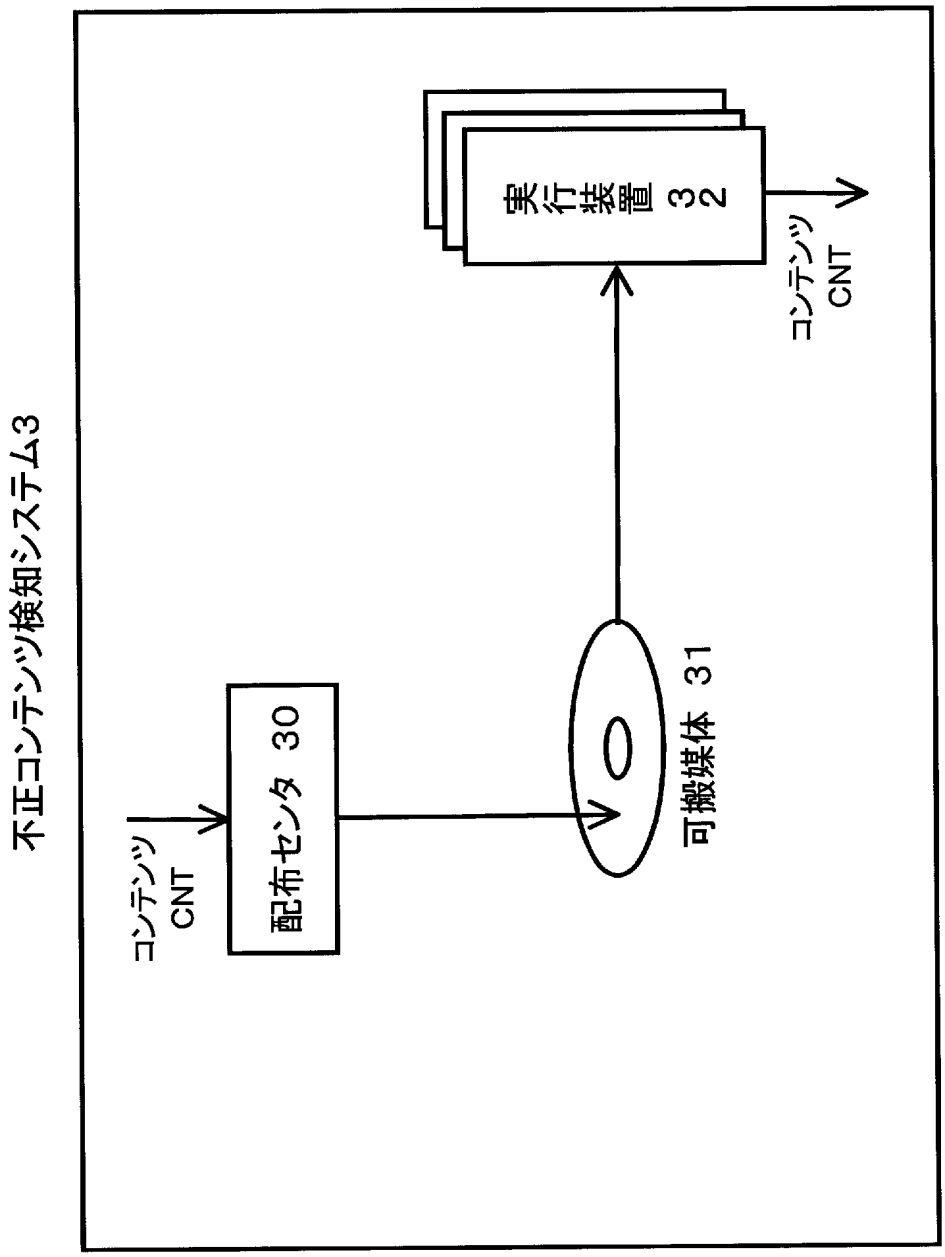
【図１８】


実行装置 22 の一例
取得部
221
コンテンツ鍵取得部
123
コンテンツ位置
情報取得部
124
認証情報検証部
126
部分復号化部
127
ヘッダ情報検証部
128
実行部
129
検証情報格納部
125
デバイス鍵格納部
122
コンテンツ
CNT

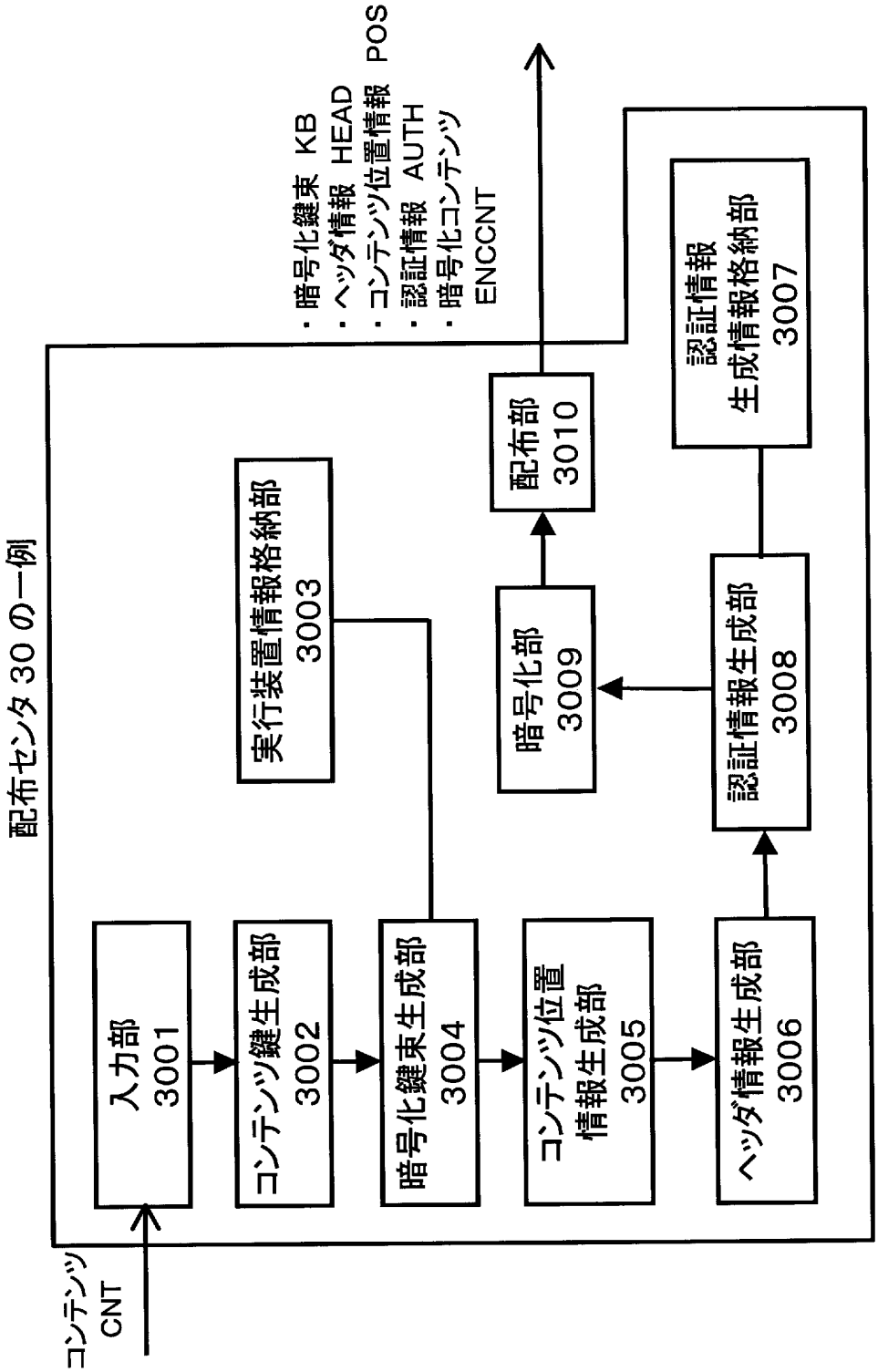
【図１９】


処理開始
ヘッダ識別子を選択し、コンテンツ鍵を取得
コンテンツ位置情報を取得
認証情報を検証
正常？
異常
正常
暗号化代表部分コンテンツを復号化
ハッシュ値を検証
正常？
異常
正常
暗号化コンテンツを復号化しながら
コンテンツを実行
処理終了
S221
S222
S223
S224
S225
S226
S227
S228

【図２０】

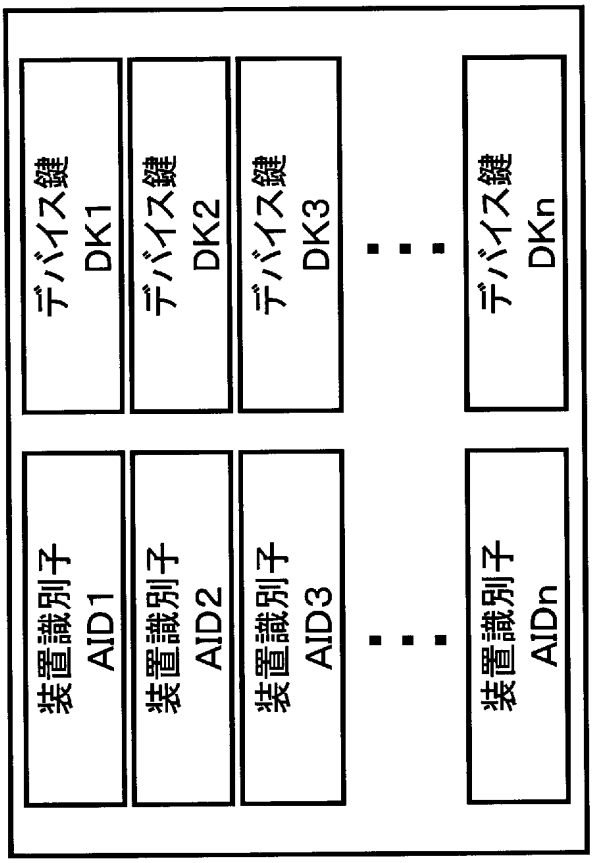


【図２１】


配布センタ 30 の一例
コンテンツ CNT
入力部 3001
コンテンツ鍵生成部 3002
暗号化鍵束生成部 3004
コンテンツ位置情報生成部 3005
ヘッダ情報生成部 3006
実行装置情報格納部 3003
暗号化部 3009
認証情報生成部 3008
配布部 3010
認証情報生成情報格納部 3007
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・コンテンツ位置情報 POS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

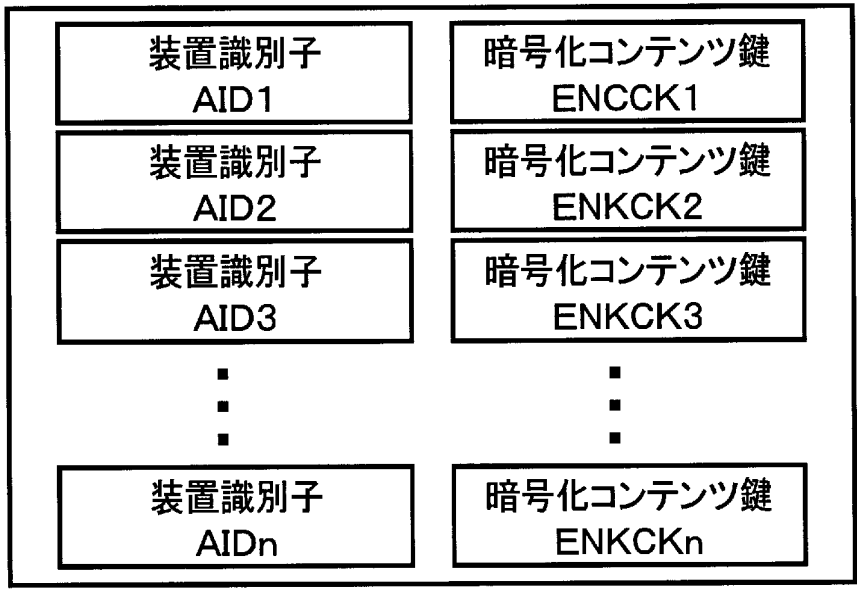
【図２２】

実行装置情報格納部3003の一例

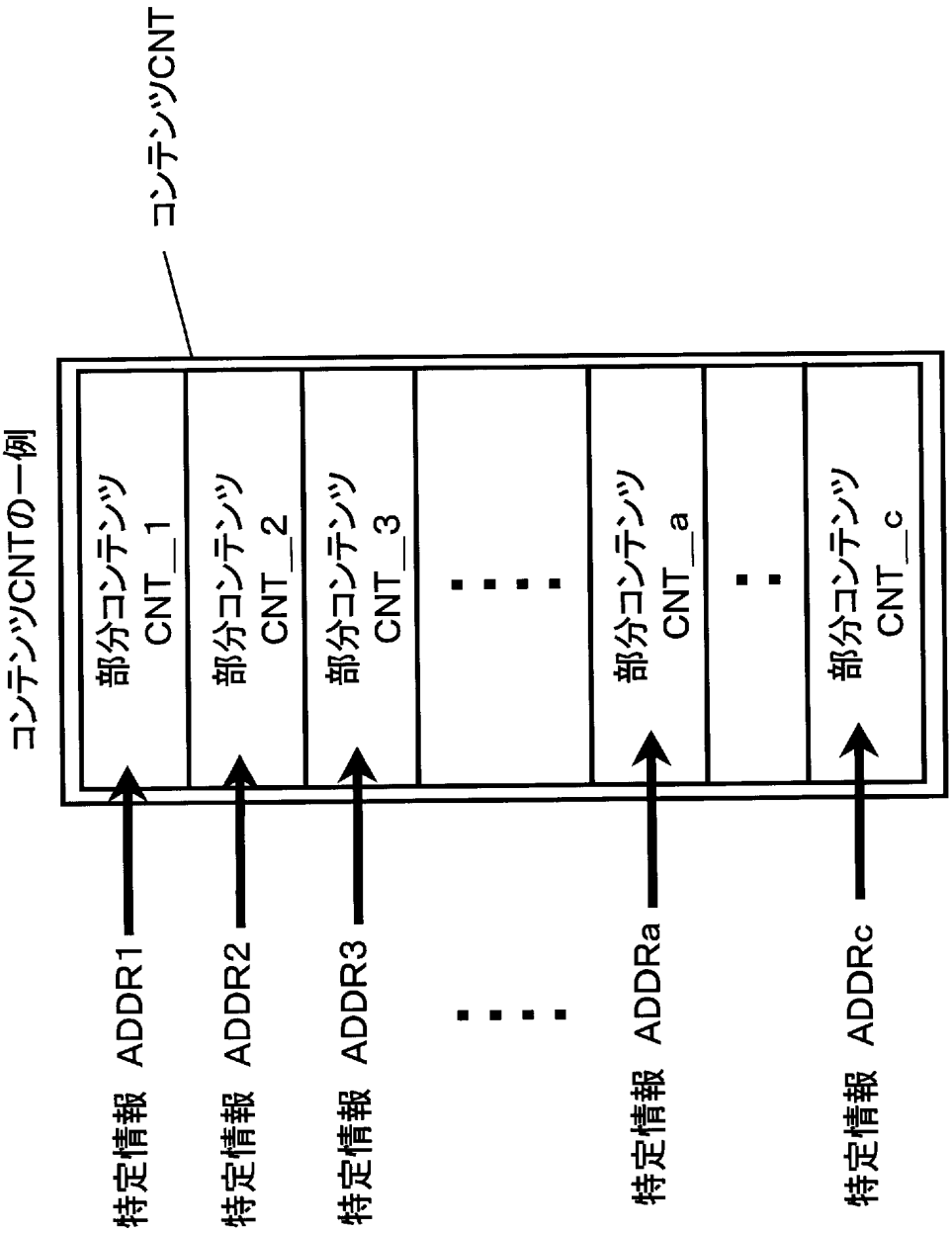


【図２３】

暗号化鍵束　KBの一例

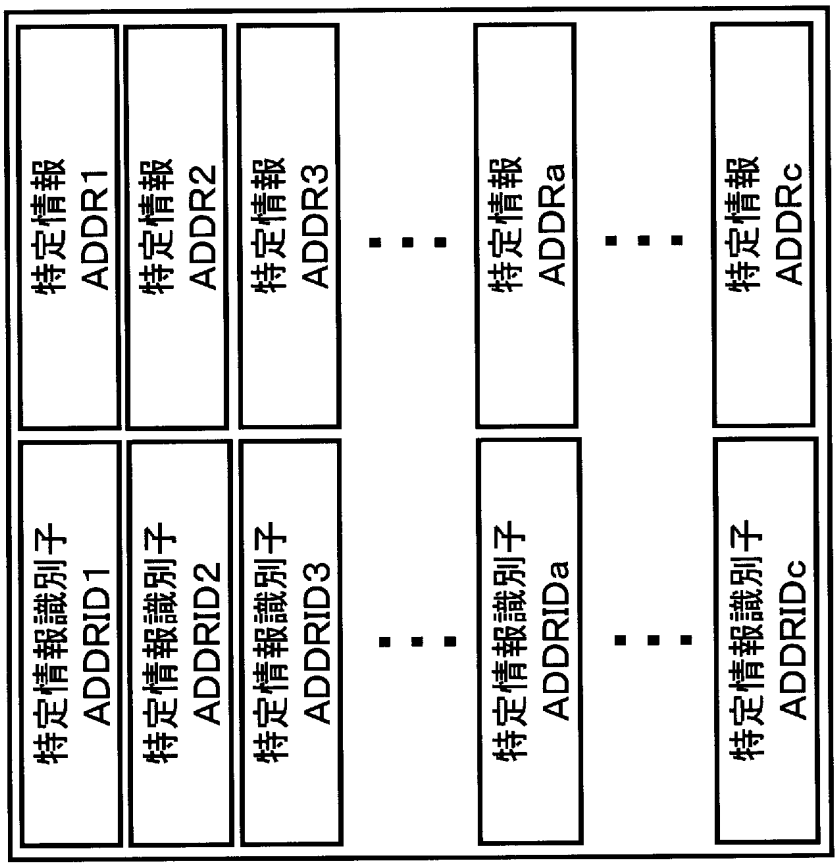


【図２４】


コンテンツCNTの一例
コンテンツCNT
部分コンテンツ CNT_1
部分コンテンツ CNT_2
部分コンテンツ CNT_3
部分コンテンツ CNT_a
部分コンテンツ CNT_c
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDR3
特定情報 ADDRa
特定情報 ADDRc

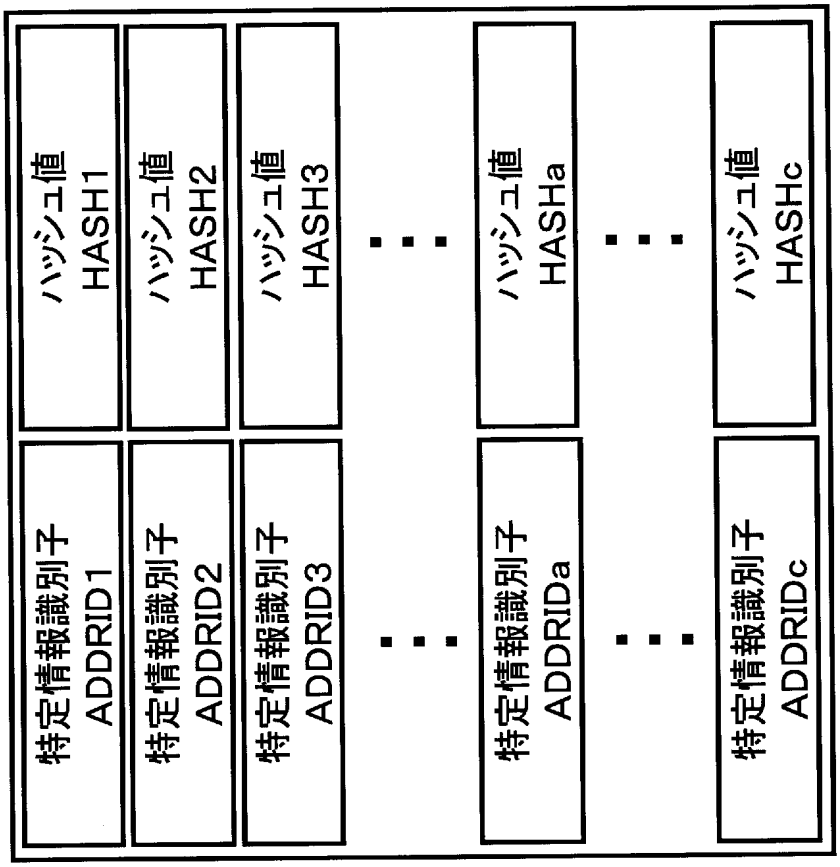
【図２５】

コンテンツ位置情報　POSの一例

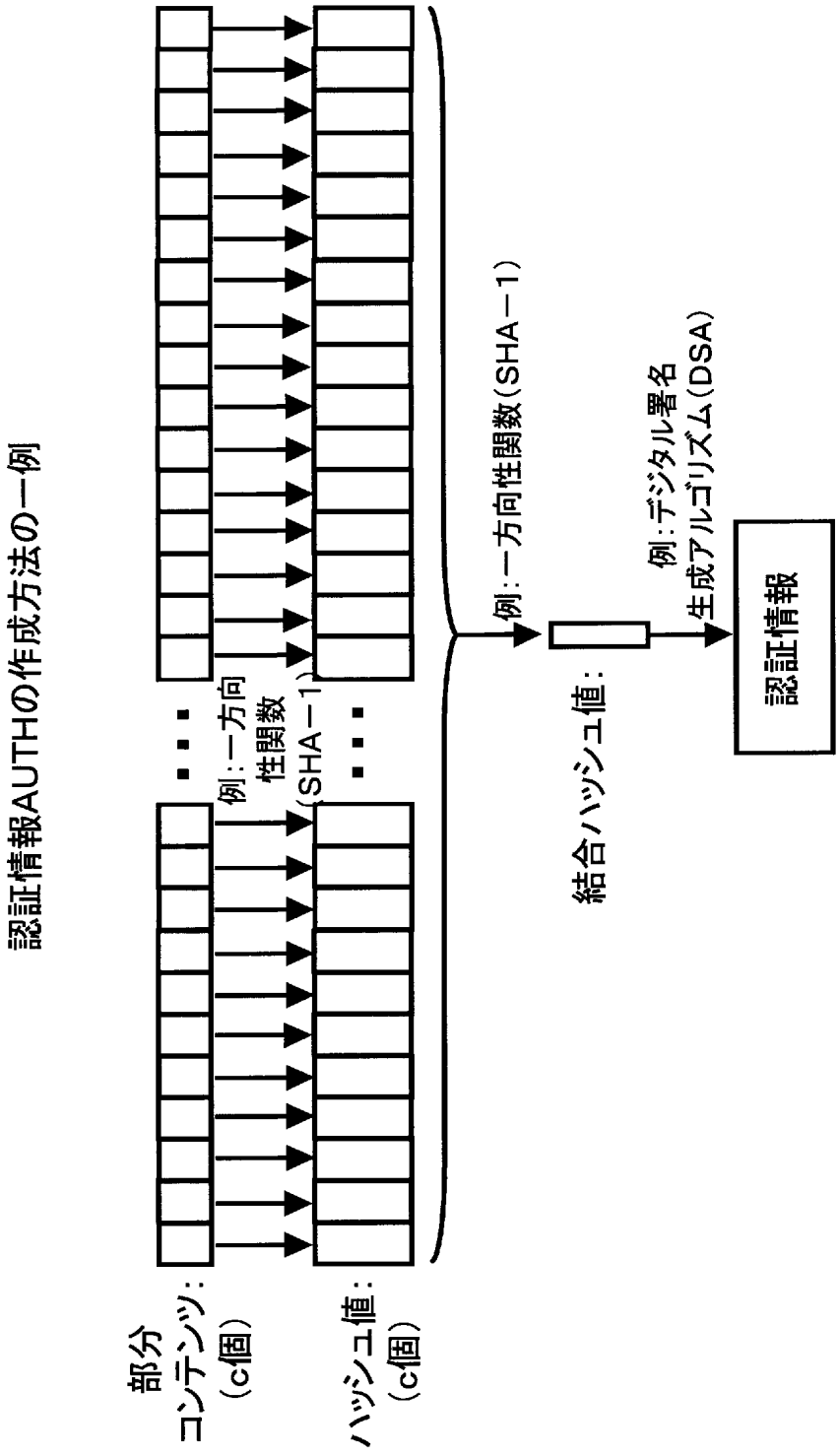


【図２６】

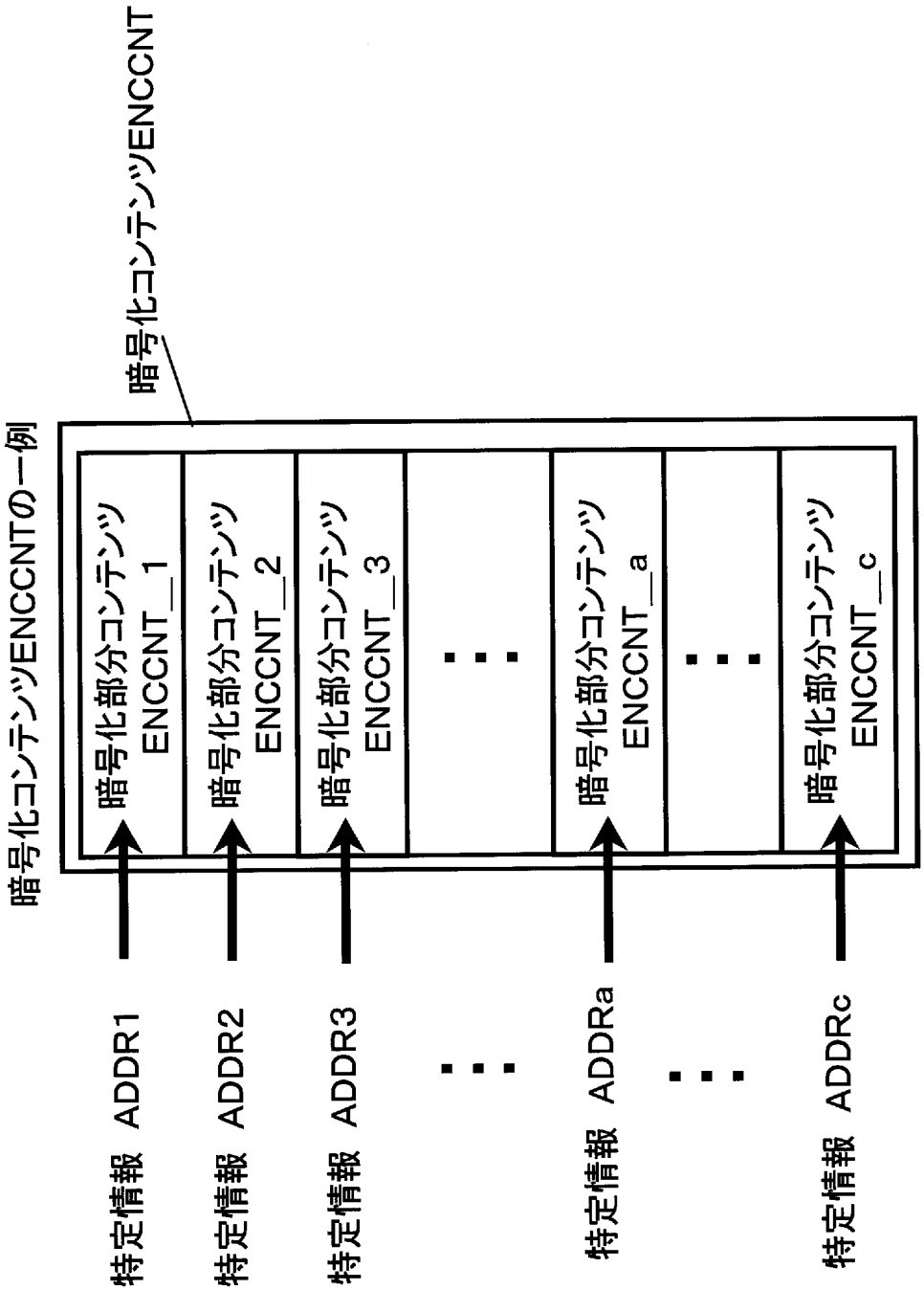
ヘッダ情報　HEADの一例



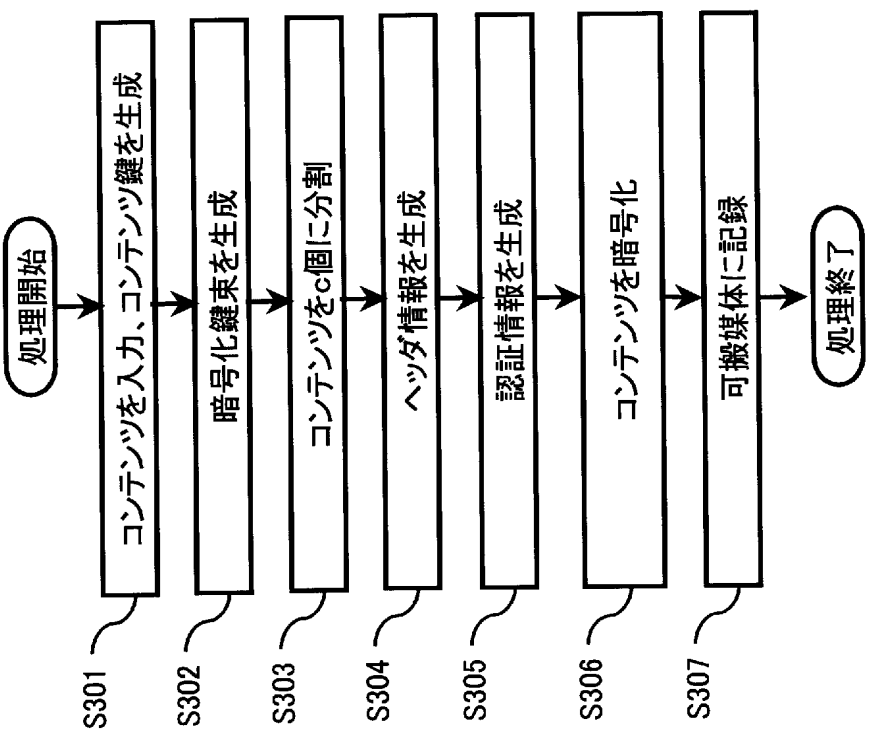
【図２７】


認証情報AUTHの作成方法の一例
部分
コンテンツ:
(c個)
例:一方向
性関数
(SHA－1)
ハッシュ値:
(c個)
例:一方向性関数(SHA－1)
結合ハッシュ値:
例:デジタル署名
生成アルゴリズム(DSA)
認証情報

【図２８】

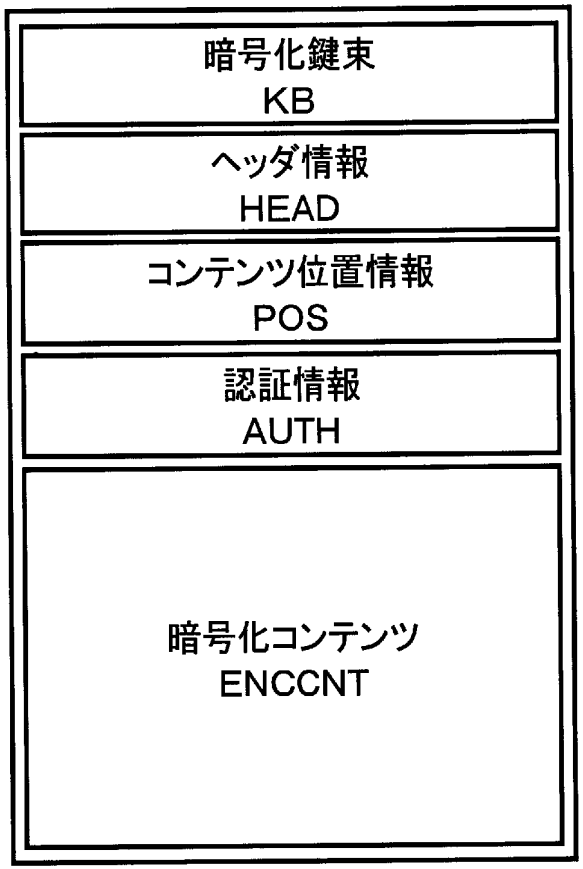

暗号化コンテンツENCCNTの一例
暗号化コンテンツENCCNT
暗号化部分コンテンツ ENCCNT_1
暗号化部分コンテンツ ENCCNT_2
暗号化部分コンテンツ ENCCNT_3
暗号化部分コンテンツ ENCCNT_a
暗号化部分コンテンツ ENCCNT_c
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDR3
特定情報 ADDRa
特定情報 ADDRc

【図２９】

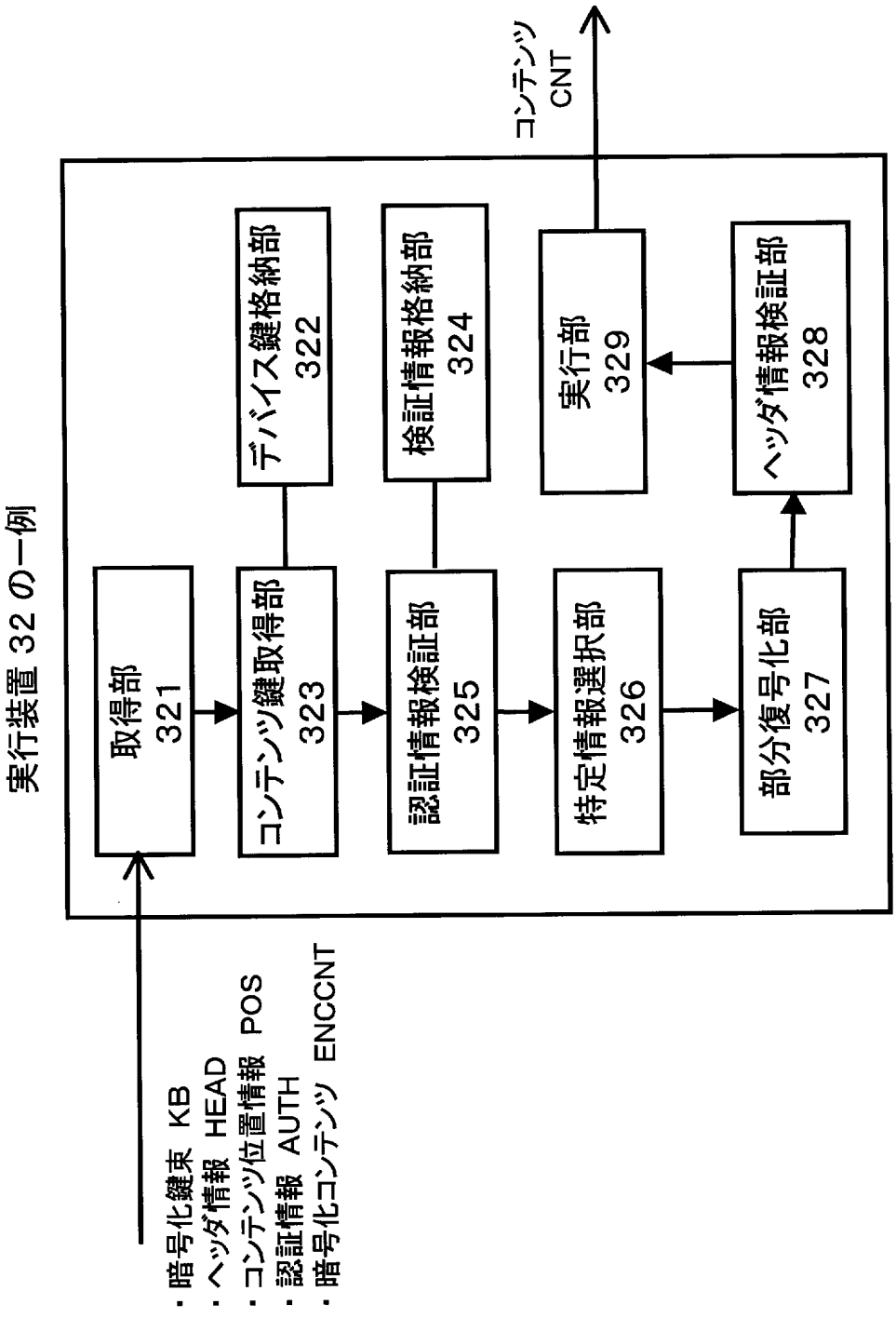

処理開始
コンテンツを入力、コンテンツ鍵を生成
暗号化鍵束を生成
コンテンツをc個に分割
ヘッダ情報を生成
認証情報を生成
コンテンツを暗号化
可搬媒体に記録
処理終了
S301
S302
S303
S304
S305
S306
S307

【図３０】

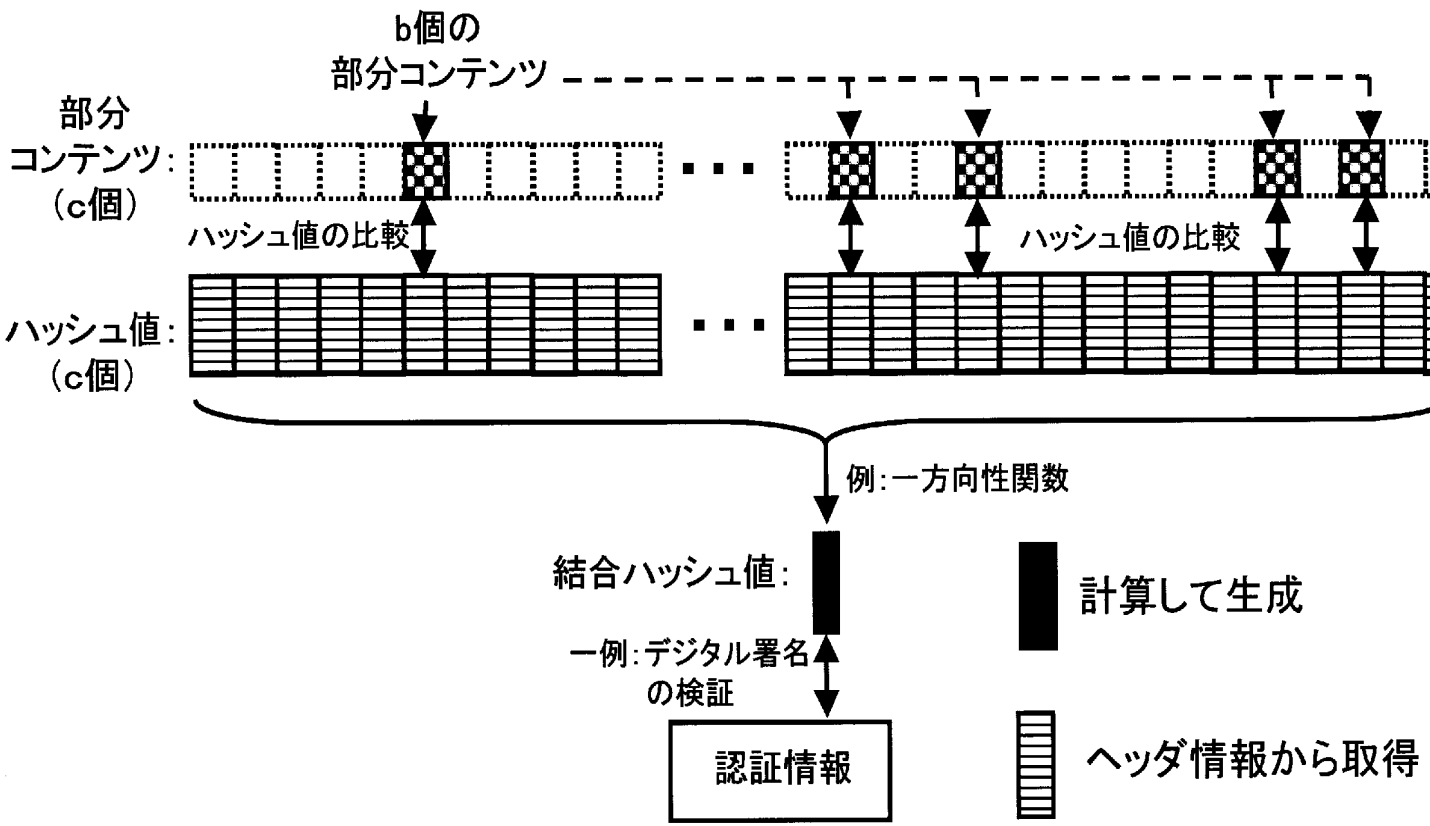
可搬媒体31に記録されるデータの一例



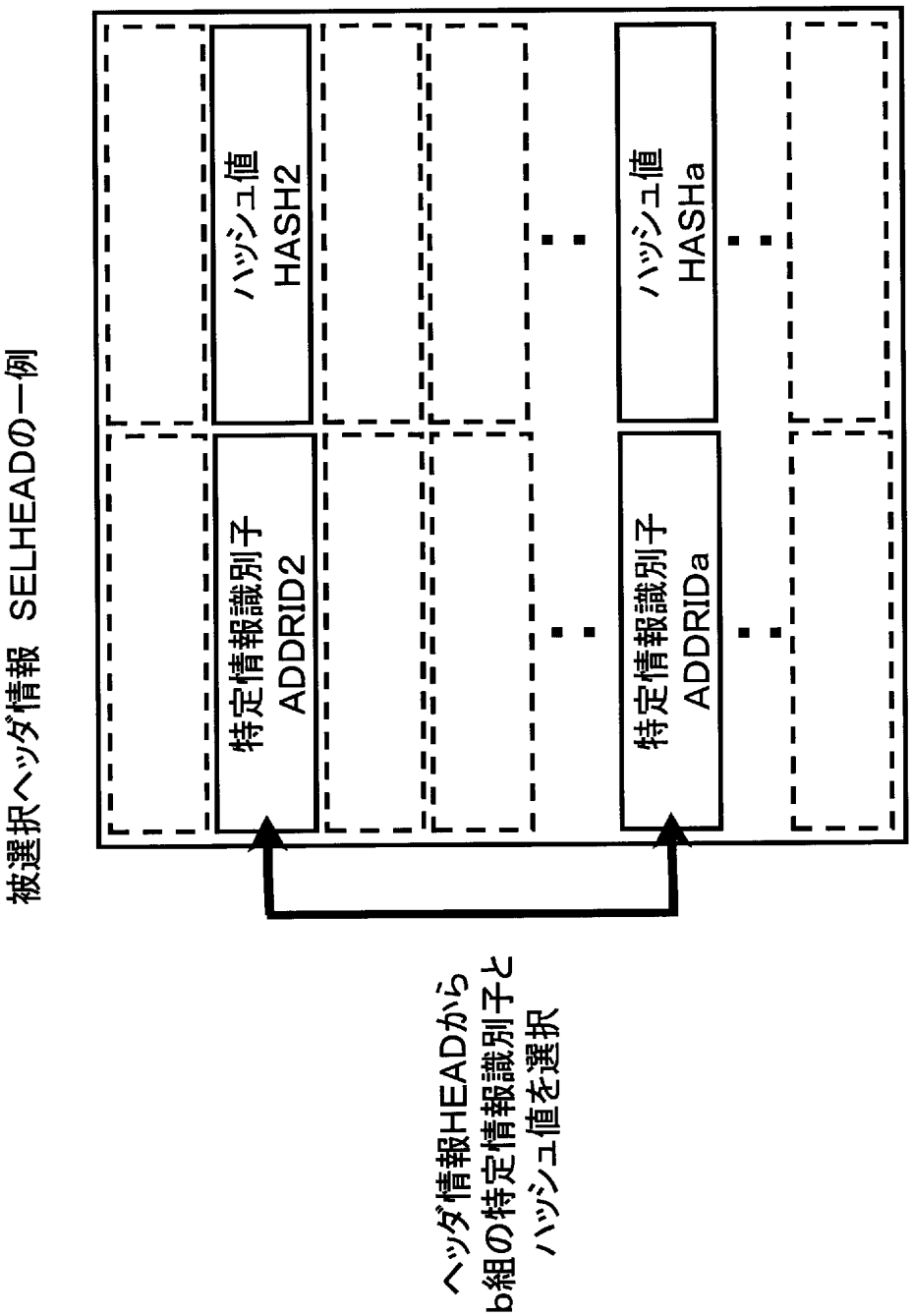
【図３１】


実行装置 32 の一例
取得部 321
コンテンツ鍵取得部 323
デバイス鍵格納部 322
認証情報検証部 325
検証情報格納部 324
特定情報選択部 326
部分復号化部 327
実行部 329
ヘッダ情報検証部 328
コンテンツ CNT
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・コンテンツ位置情報 POS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

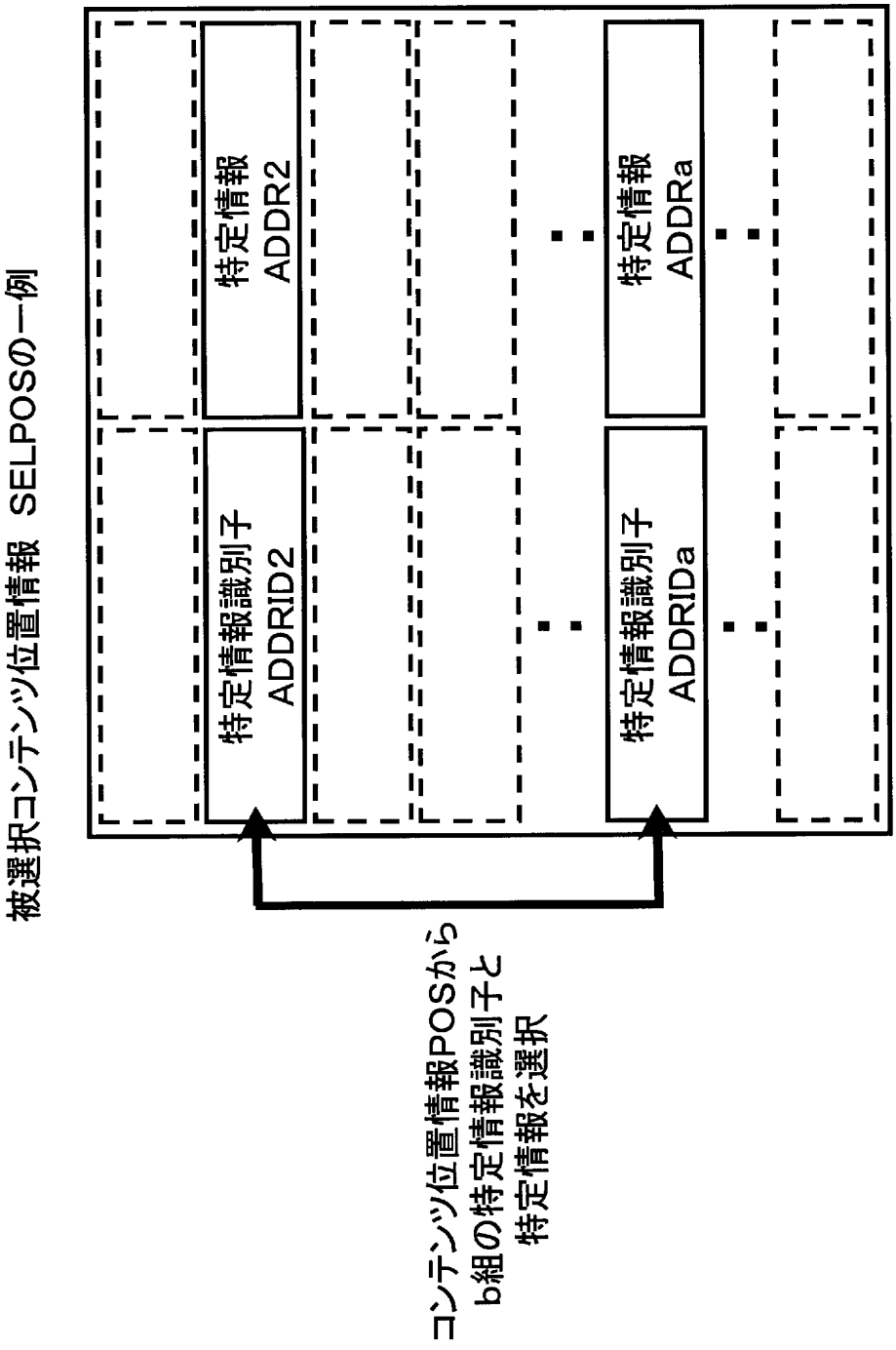
認証情報検証部325、及び、ヘッダ情報検証部328の動作の一例



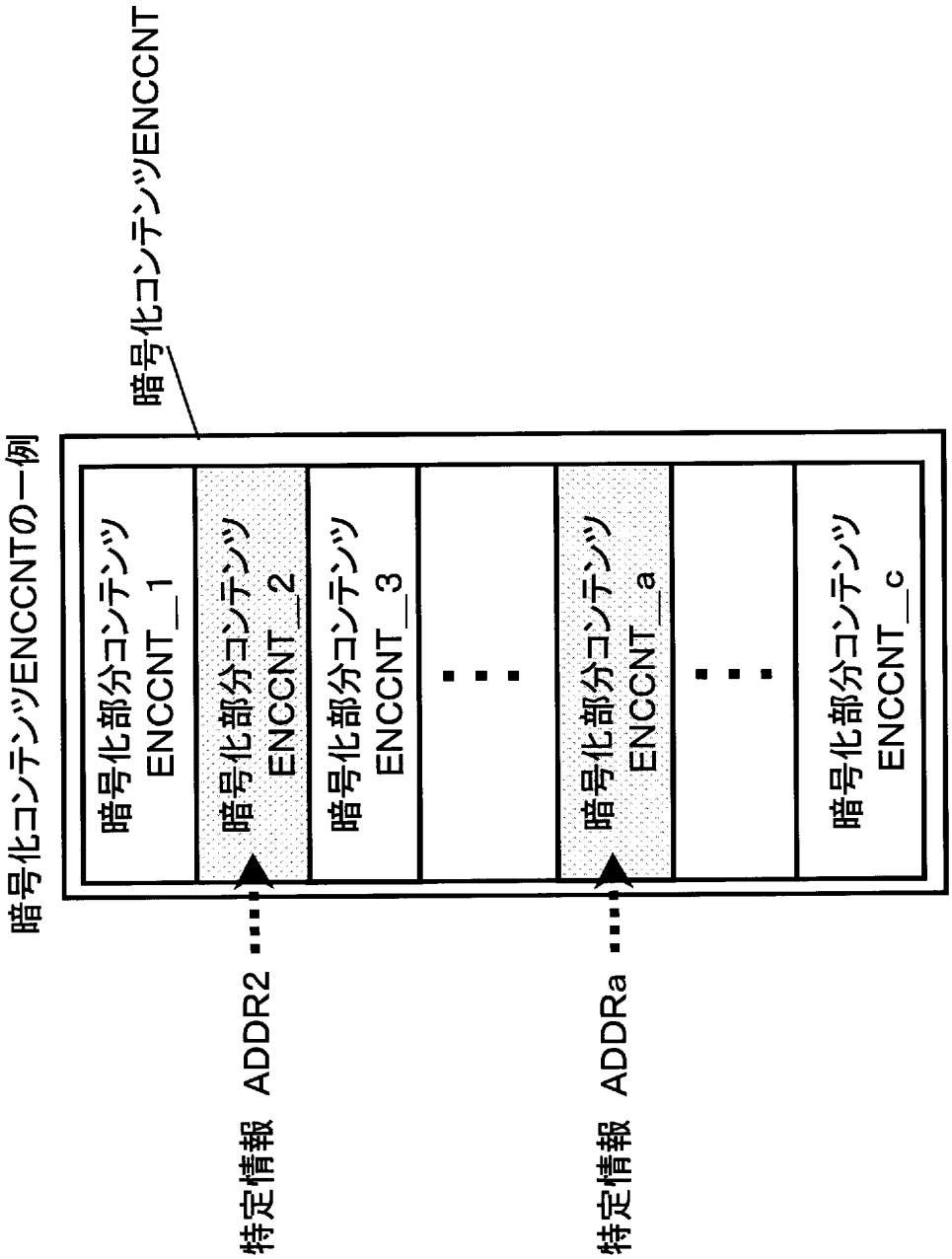
【図３３】


被選択ヘッダ情報　SELHEADの一例
特定情報識別子
ADDRID2
ハッシュ値
HASH2
特定情報識別子
ADDRIDa
ハッシュ値
HASHa
ヘッダ情報HEADから
b組の特定情報識別子と
ハッシュ値を選択

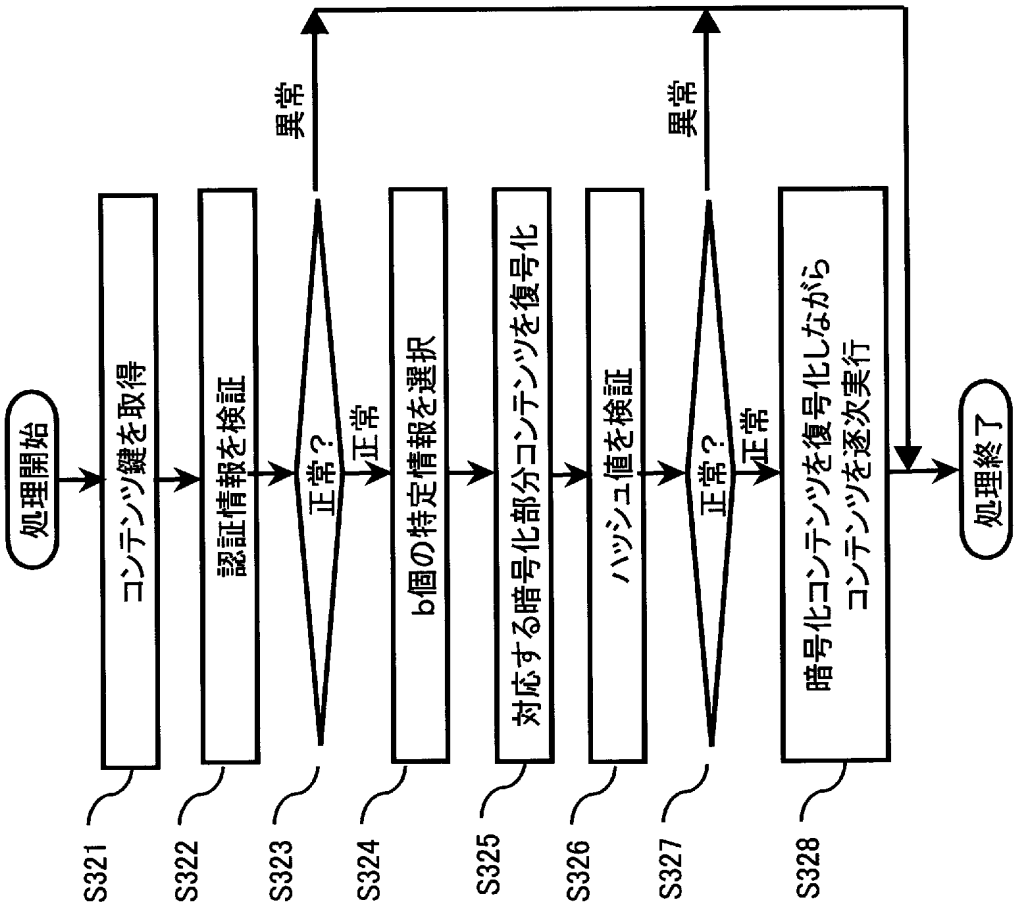
【図３４】


被選択コンテンツ位置情報　SELPOSの一例
特定情報識別子
ADDRID2
特定情報
ADDR2
特定情報識別子
ADDRIDa
特定情報
ADDRa
コンテンツ位置情報POSから
b組の特定情報識別子と
特定情報を選択

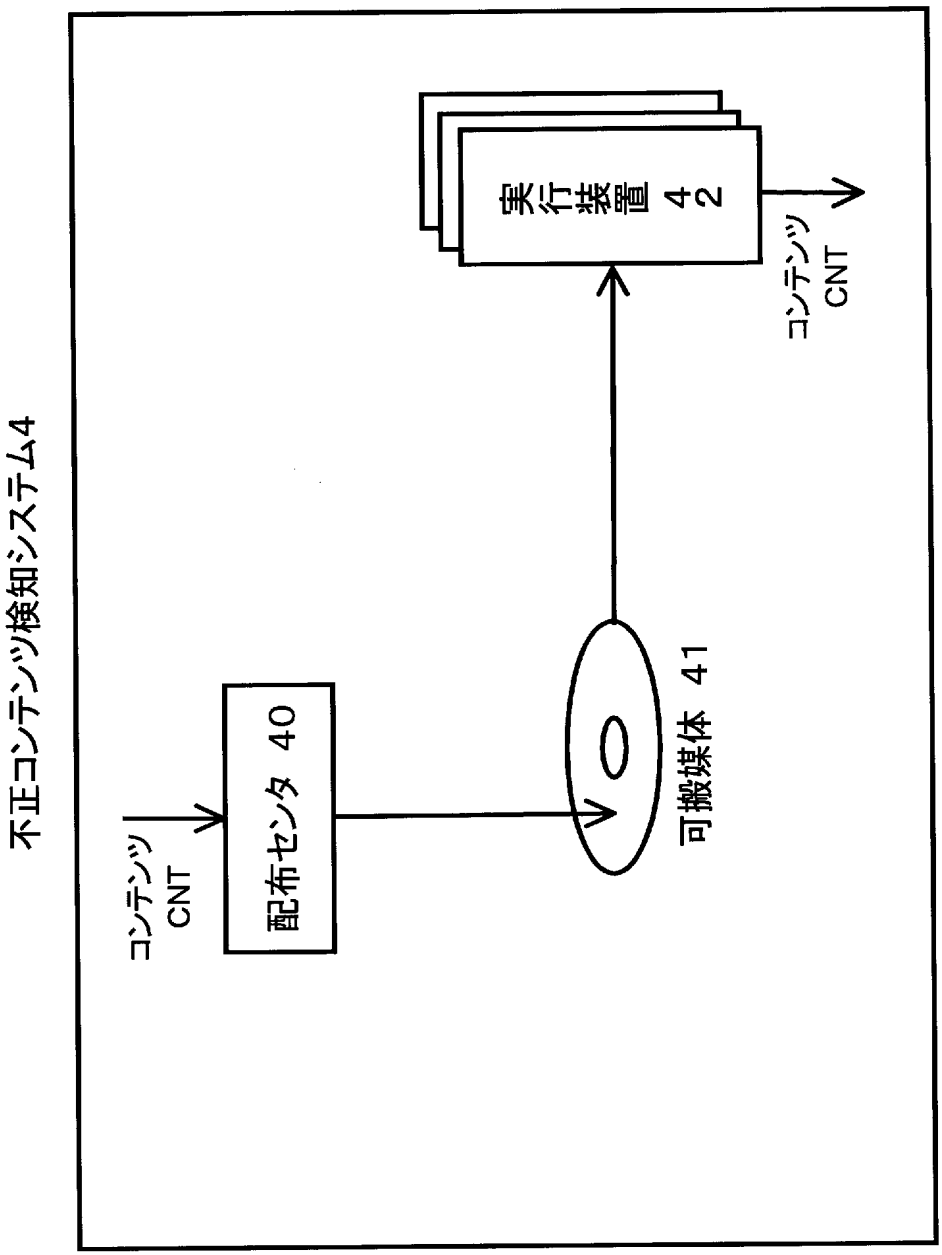
【図３５】


暗号化コンテンツENCCNTの一例
暗号化コンテンツENCCNT
暗号化部分コンテンツ ENCCNT_1
暗号化部分コンテンツ ENCCNT_2
暗号化部分コンテンツ ENCCNT_3
暗号化部分コンテンツ ENCCNT_a
暗号化部分コンテンツ ENCCNT_c
特定情報 ADDR2
特定情報 ADDRa

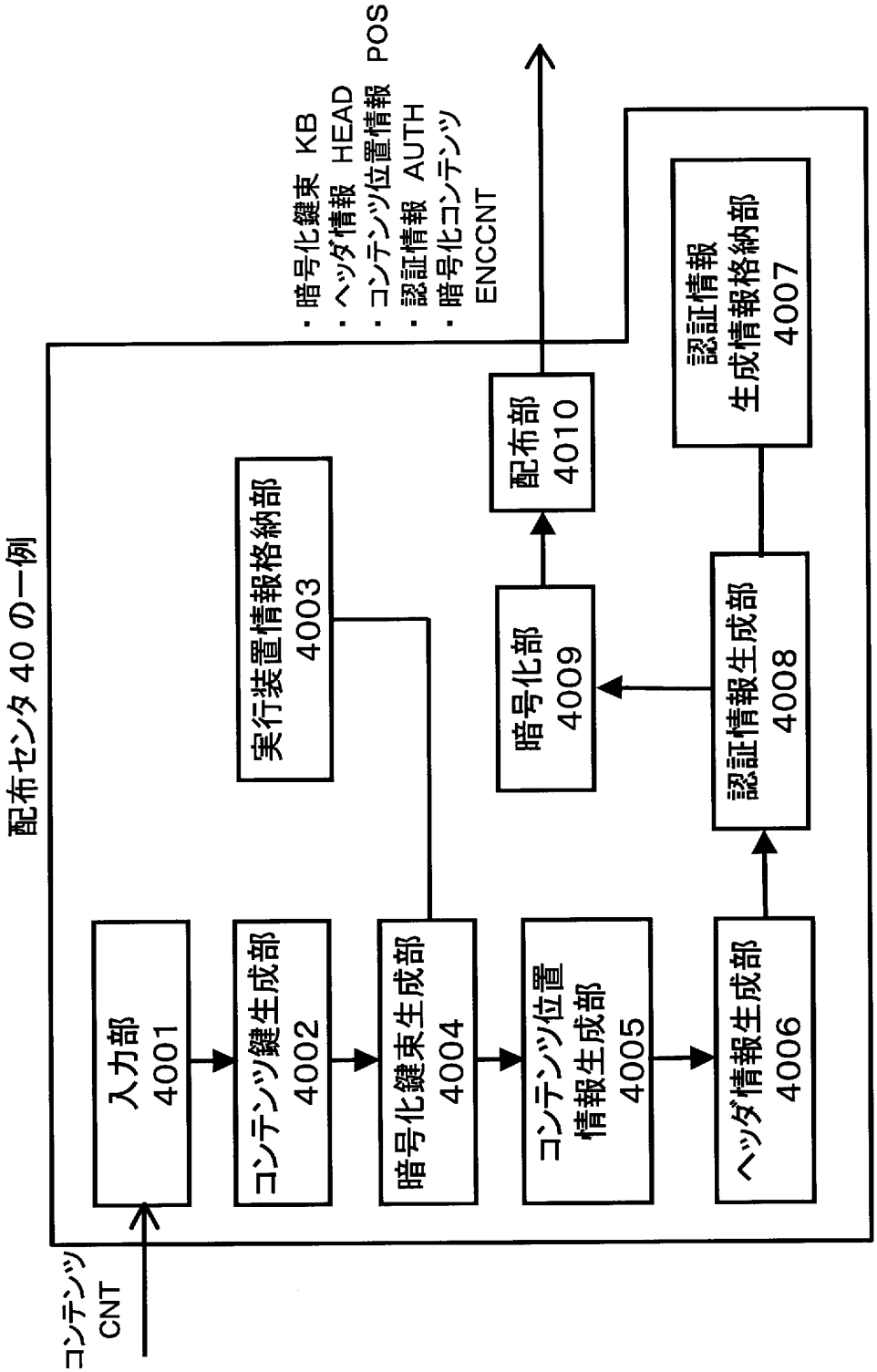
【図３６】


処理開始
コンテンツ鍵を取得
認証情報を検証
正常？
異常
正常
b個の特定情報を選択
対応する暗号化部分コンテンツを復号化
ハッシュ値を検証
正常？
異常
正常
暗号化コンテンツを復号化しながら
コンテンツを逐次実行
処理終了
S321
S322
S323
S324
S325
S326
S327
S328

【図３７】

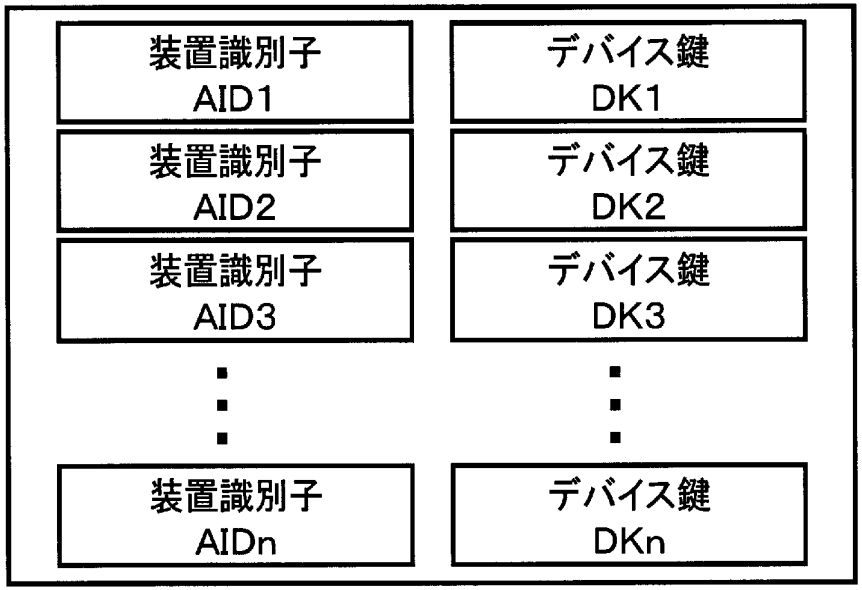


【図３８】


配布センタ 40 の一例
コンテンツ CNT
入力部 4001
コンテンツ鍵生成部 4002
暗号化鍵束生成部 4004
コンテンツ位置情報生成部 4005
ヘッダ情報生成部 4006
実行装置情報格納部 4003
暗号化部 4009
認証情報生成部 4008
配布部 4010
認証情報生成部格納部 4007
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・コンテンツ位置情報 POS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

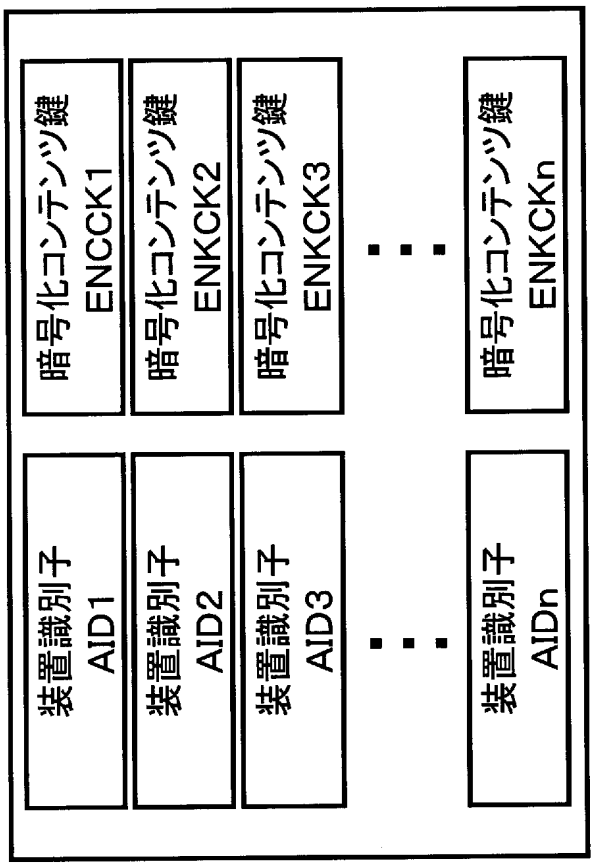
【図３９】

実行装置情報格納部4003の一例

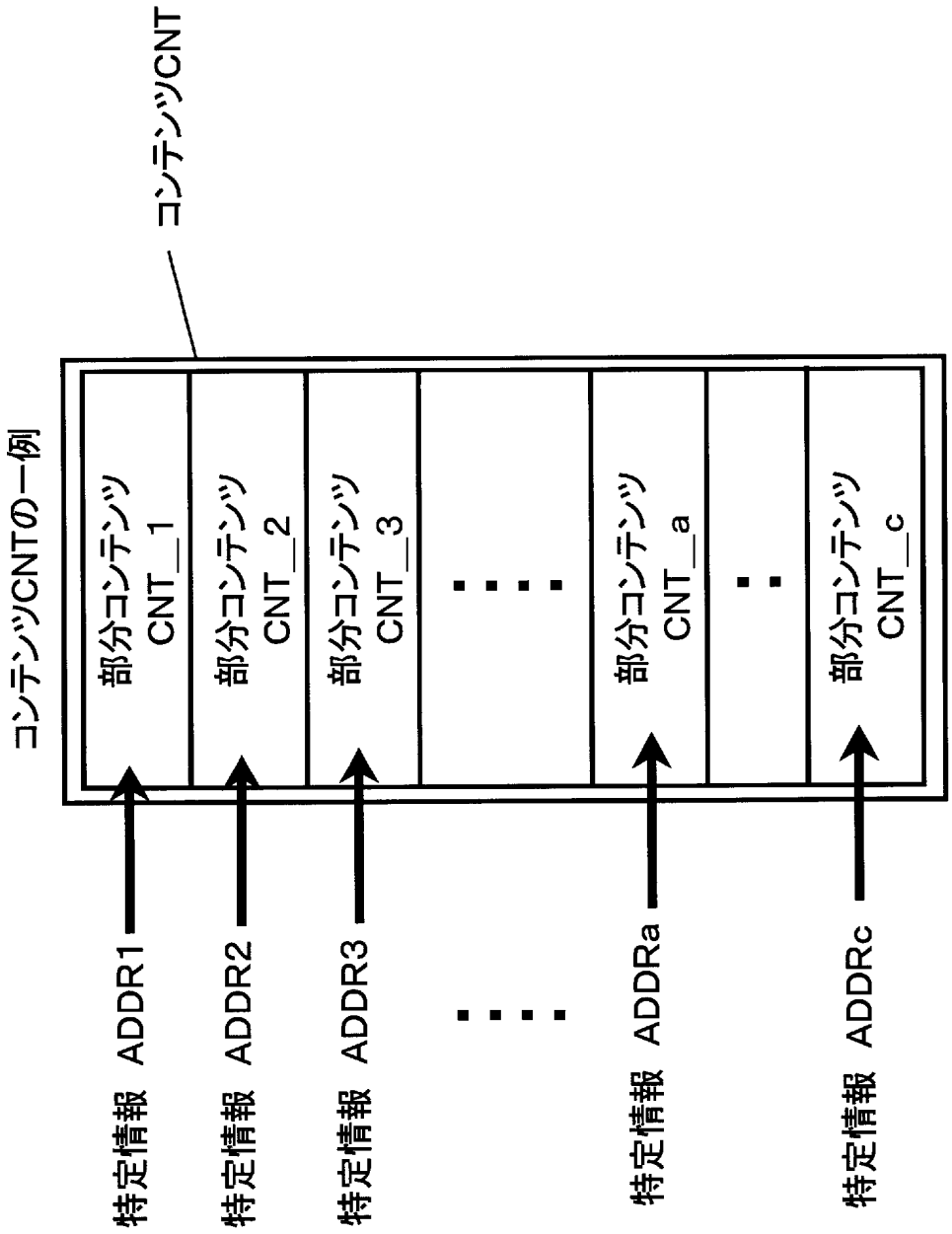


【図４０】

暗号化鍵束　KBの一例

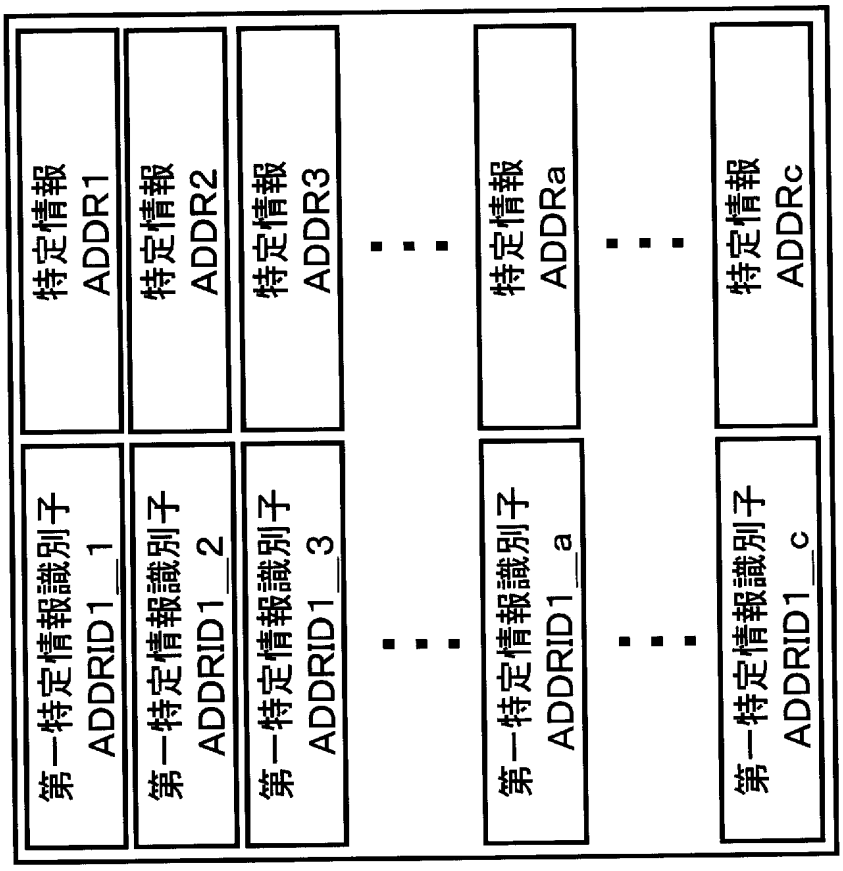


【図４１】

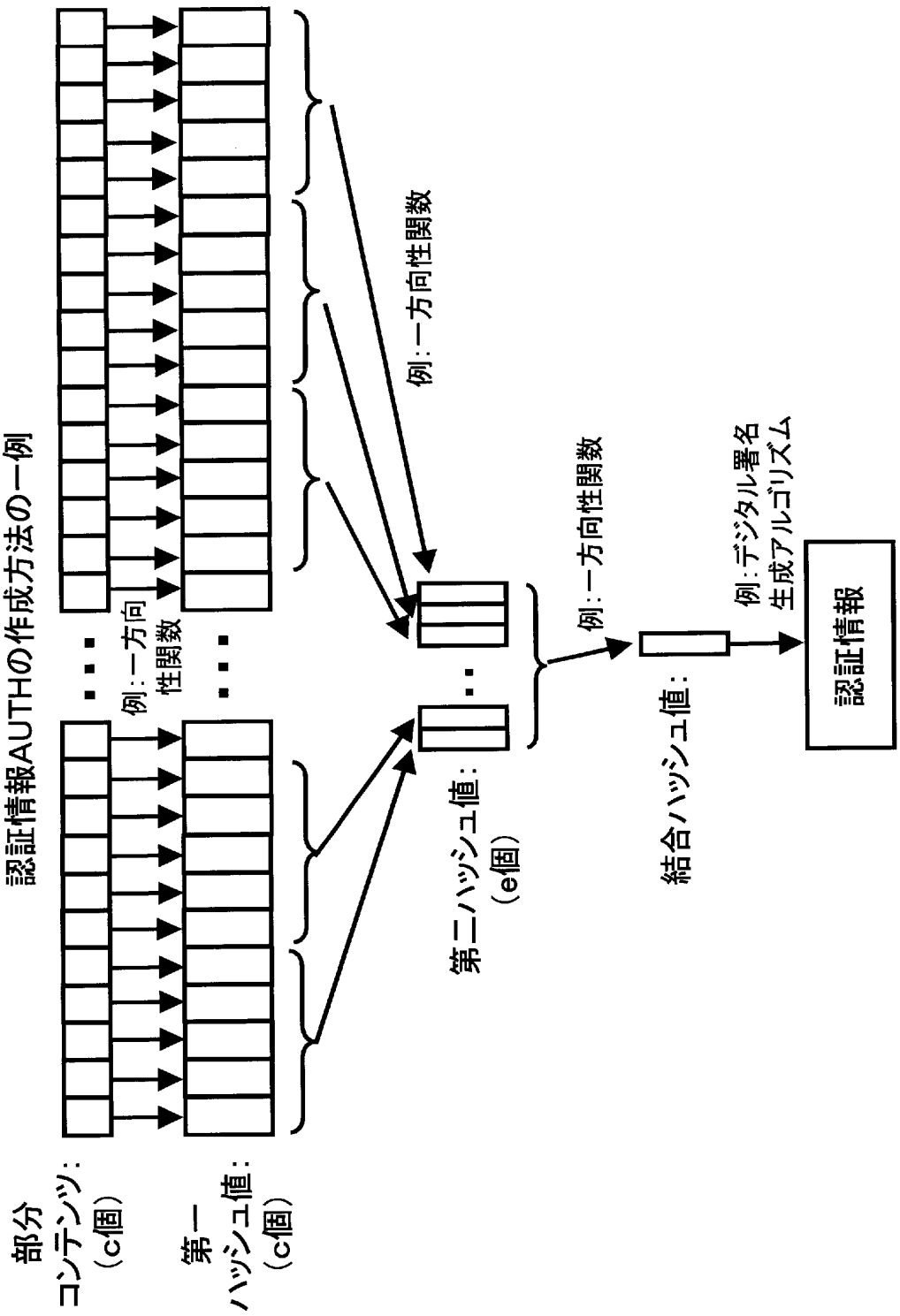

コンテンツCNTの一例
コンテンツCNT
部分コンテンツ CNT_1
部分コンテンツ CNT_2
部分コンテンツ CNT_3
部分コンテンツ CNT_a
部分コンテンツ CNT_c
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDR3
特定情報 ADDRa
特定情報 ADDRc

【図４２】

コンテンツ位置情報　POSの一例

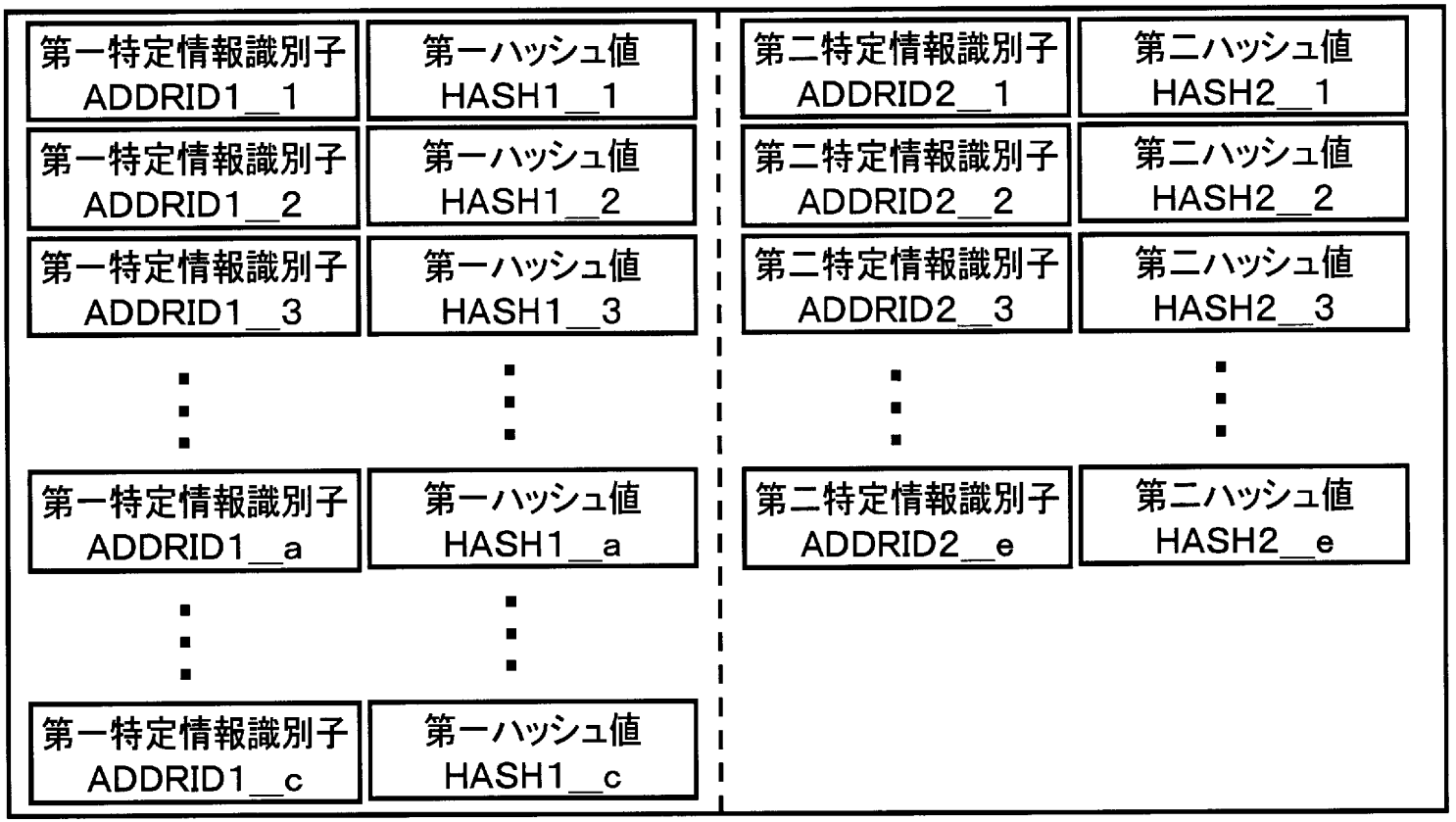


【図４３】

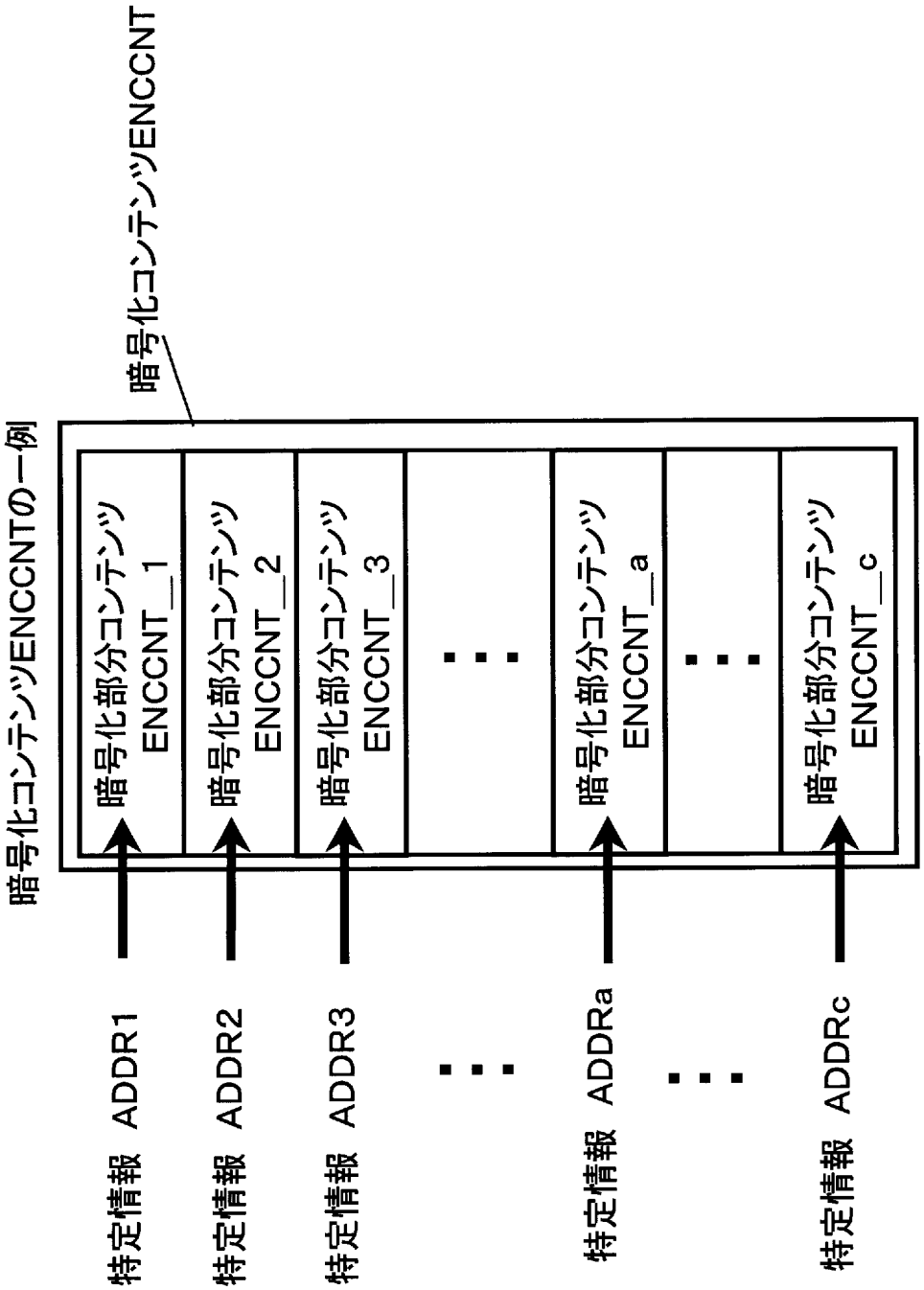

認証情報AUTHの作成方法の一例
部分
コンテンツ:
(c個)
第一
ハッシュ値:
(c個)
例:一方向
性関数
例:一方向性関数
第二ハッシュ値:
(e個)
例:一方向性関数
結合ハッシュ値:
例:デジタル署名
生成アルゴリズム
認証情報

【図４４】

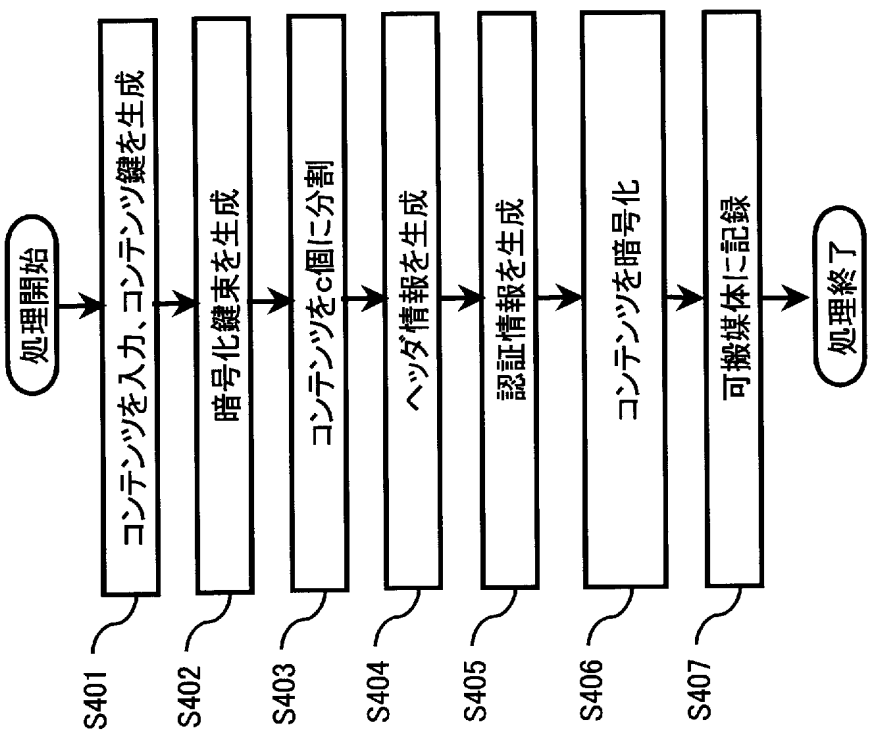
ヘッダ情報　HEADの一例



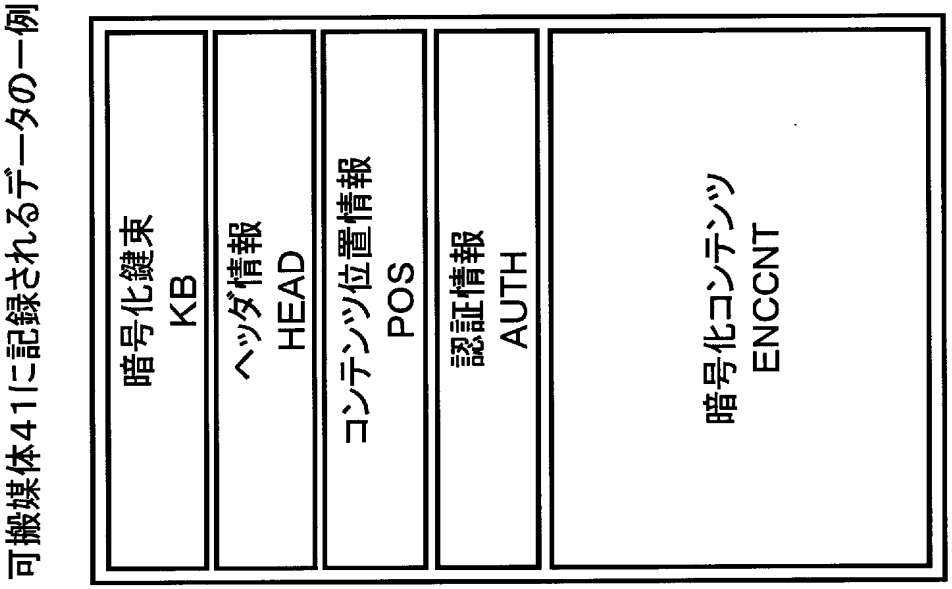
【図４５】


暗号化コンテンツENCCNTの一例
暗号化コンテンツENCCNT
暗号化部分コンテンツ ENCCNT_1
暗号化部分コンテンツ ENCCNT_2
暗号化部分コンテンツ ENCCNT_3
暗号化部分コンテンツ ENCCNT_a
暗号化部分コンテンツ ENCCNT_c
特定情報 ADDR1
特定情報 ADDR2
特定情報 ADDR3
特定情報 ADDRa
特定情報 ADDRc

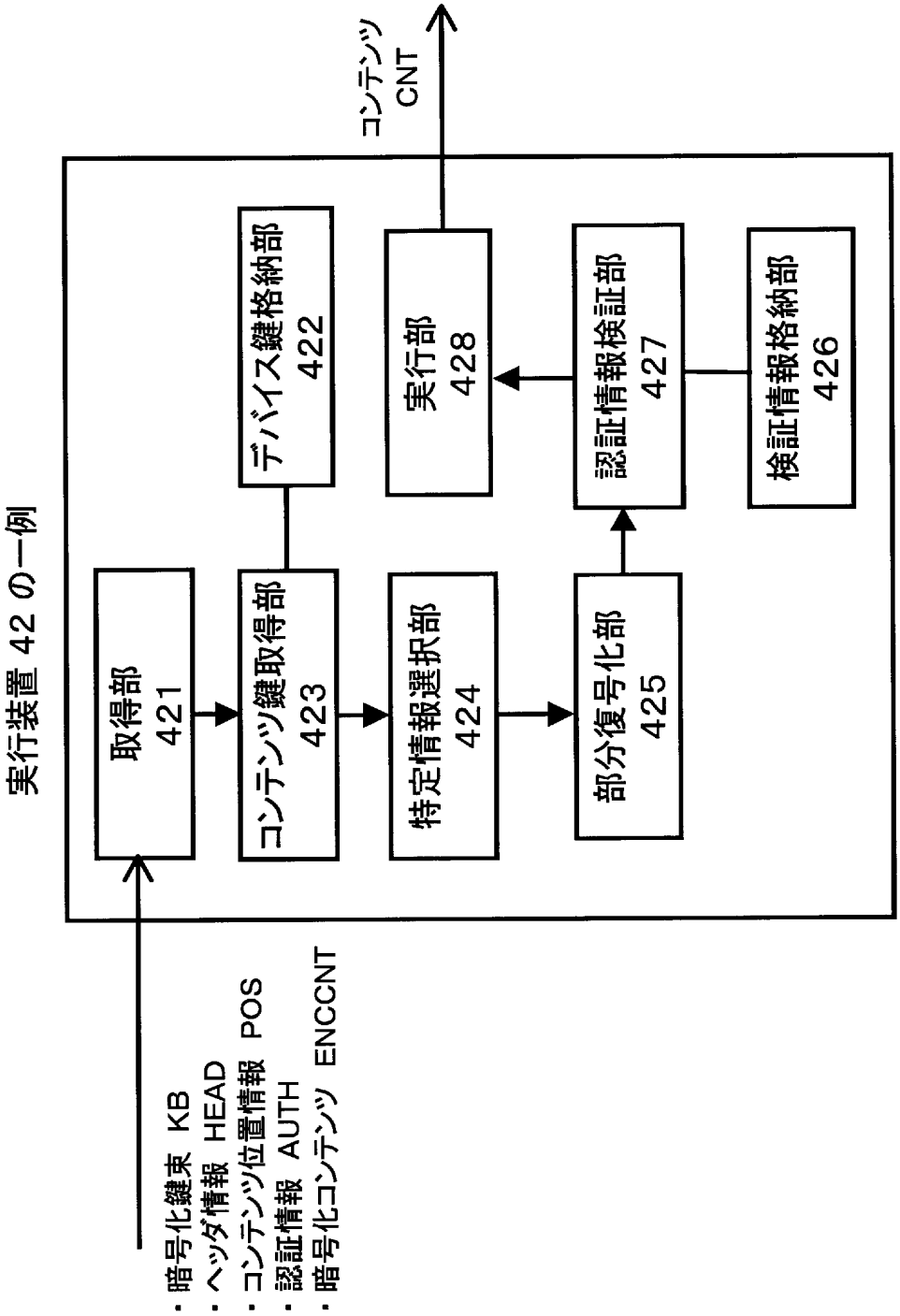
【図４６】


処理開始
コンテンツを入力、コンテンツ鍵を生成
暗号化鍵束を生成
コンテンツをc個に分割
ヘッダ情報を生成
認証情報を生成
コンテンツを暗号化
可搬媒体に記録
処理終了
S401
S402
S403
S404
S405
S406
S407

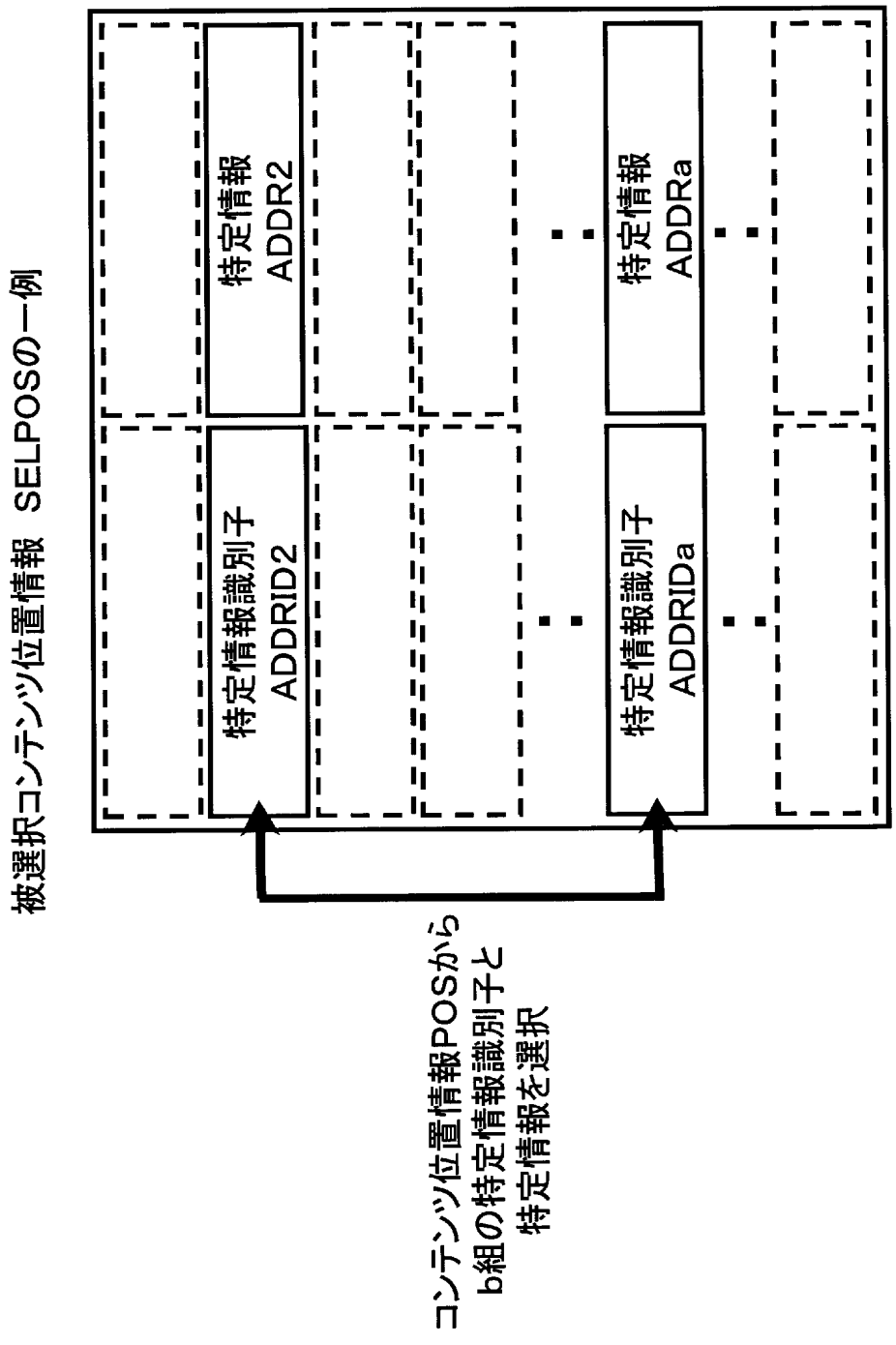
【図４７】


可搬媒体41に記録されるデータの一例
暗号化鍵束
KB
ヘッダ情報
HEAD
コンテンツ位置情報
POS
認証情報
AUTH
暗号化コンテンツ
ENCCNT

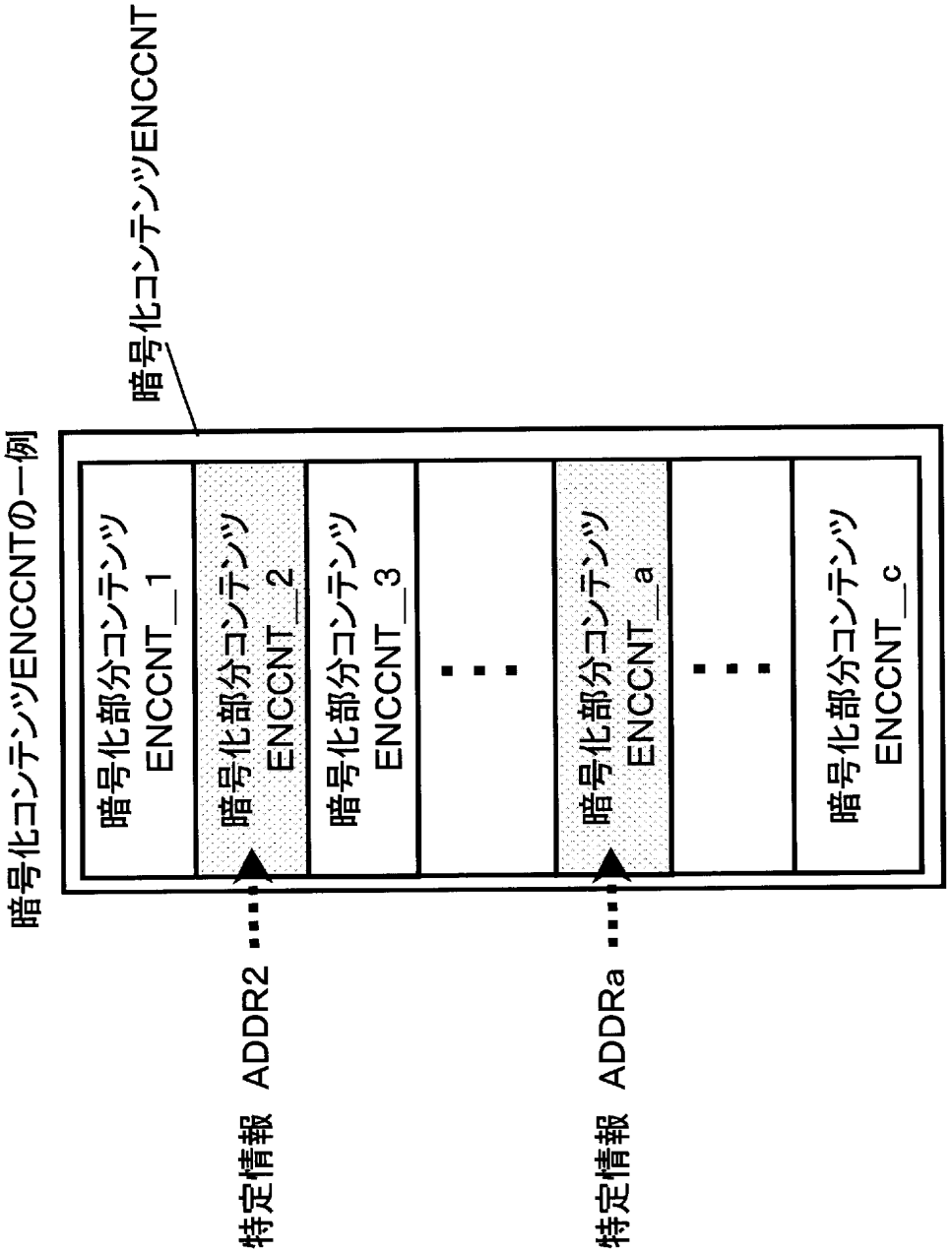
【図４８】


実行装置 42 の一例
取得部 421
コンテンツ鍵取得部 423
特定情報選択部 424
部分復号化部 425
デバイス鍵格納部 422
実行部 428
認証情報検証部 427
検証情報格納部 426
コンテンツ CNT
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・コンテンツ位置情報 POS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

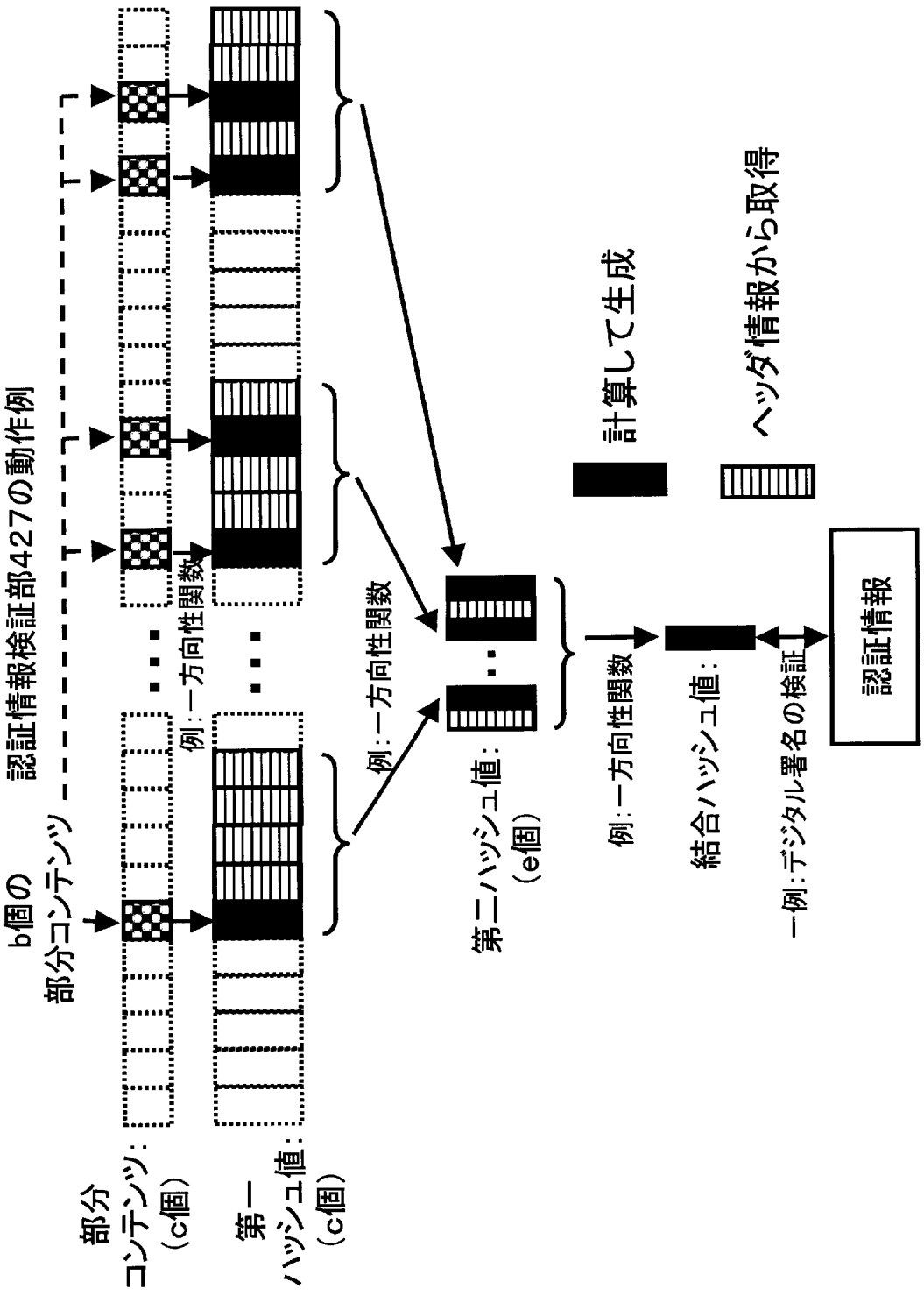
【図４９】


被選択コンテンツ位置情報　SELPOSの一例
特定情報識別子
ADDRID2
特定情報
ADDR2
特定情報識別子
ADDRIDa
特定情報
ADDRa
コンテンツ位置情報POSから
b組の特定情報識別子と
特定情報を選択

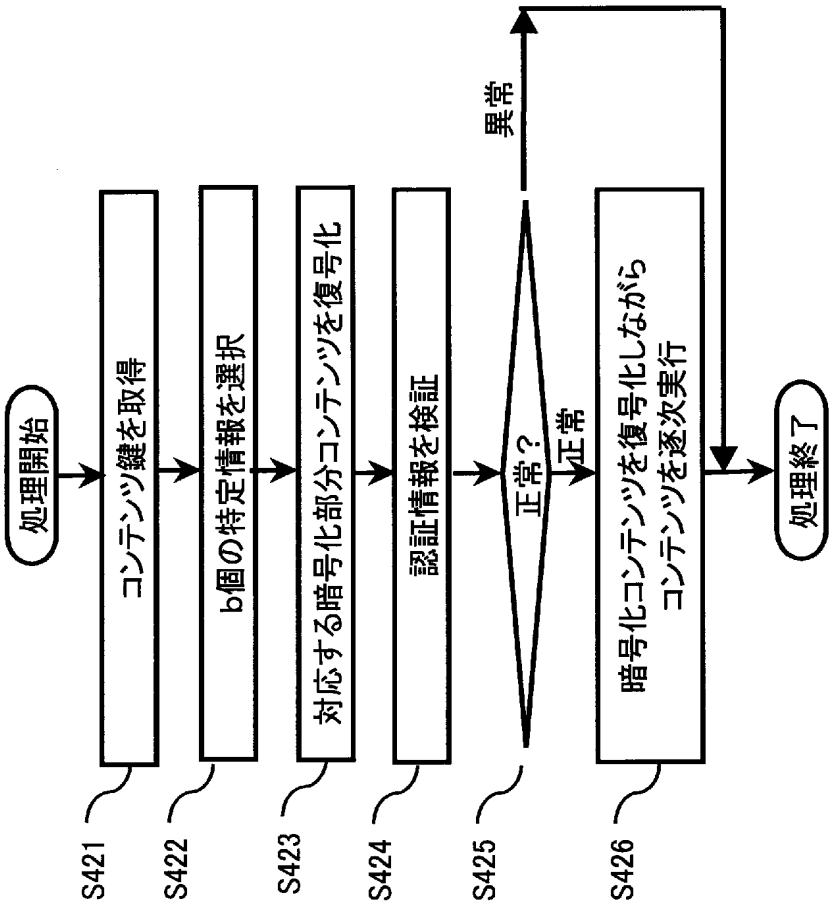
【図５０】


暗号化コンテンツENCCNTの一例
暗号化コンテンツENCCNT
暗号化部分コンテンツ ENCCNT_1
暗号化部分コンテンツ ENCCNT_2
暗号化部分コンテンツ ENCCNT_3
暗号化部分コンテンツ ENCCNT_a
暗号化部分コンテンツ ENCCNT_c
特定情報 ADDR2
特定情報 ADDRa

【図５１】

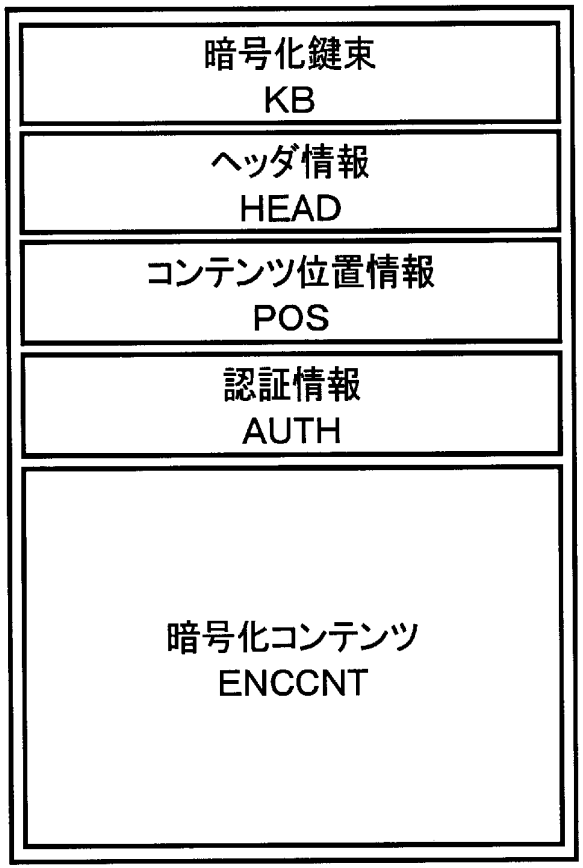

認証情報検証部427の動作例
b個の
部分コンテンツ
部分
コンテンツ:
(c個)
例:一方向性関数
第一
ハッシュ値:
(c個)
例:一方向性関数
第二ハッシュ値:
(e個)
例:一方向性関数
計算して生成
結合ハッシュ値:
ヘッダ情報から取得
一例:デジタル署名の検証
認証情報

【図５２】

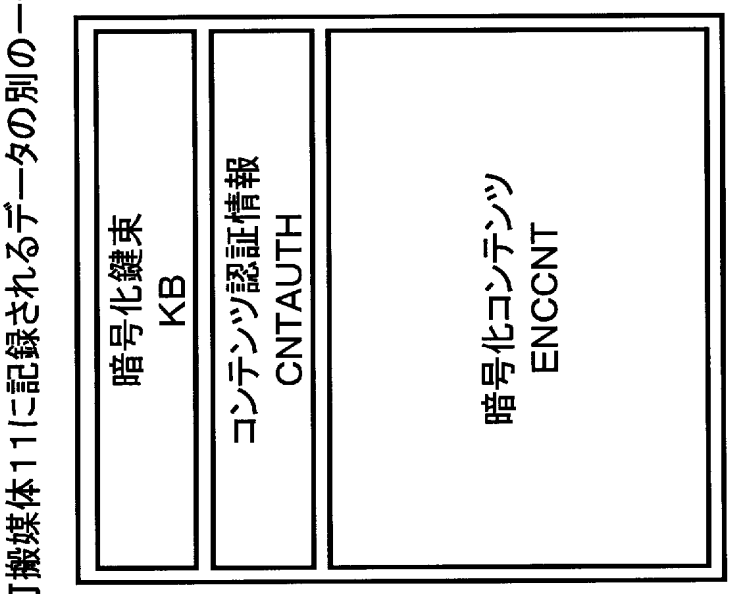

処理開始
コンテンツ鍵を取得
b個の特定情報を選択
対応する暗号化部分コンテンツを復号化
認証情報を検証
正常？
異常
正常
暗号化コンテンツを復号化しながら
コンテンツを逐次実行
処理終了
S421
S422
S423
S424
S425
S426

【図５３】

可搬媒体に記録されるデータの別の一例

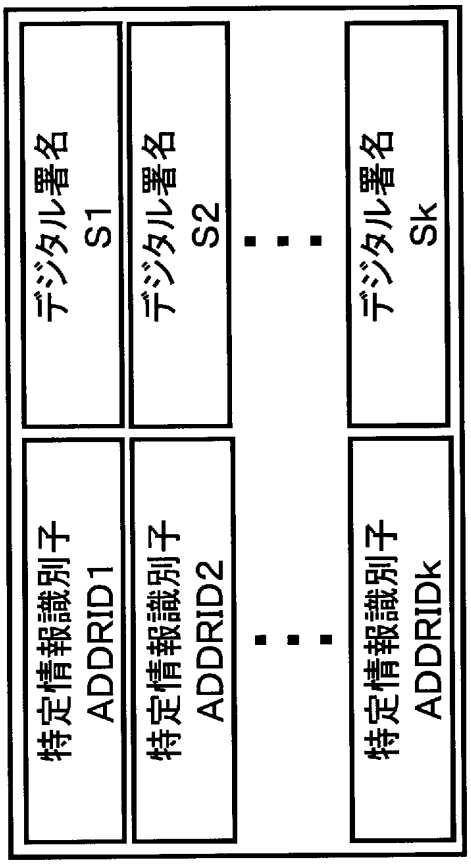


【図５４】


可搬媒体11に記録されるデータの別の一例
暗号化鍵束
KB
コンテンツ認証情報
CNTAUTH
暗号化コンテンツ
ENCCNT

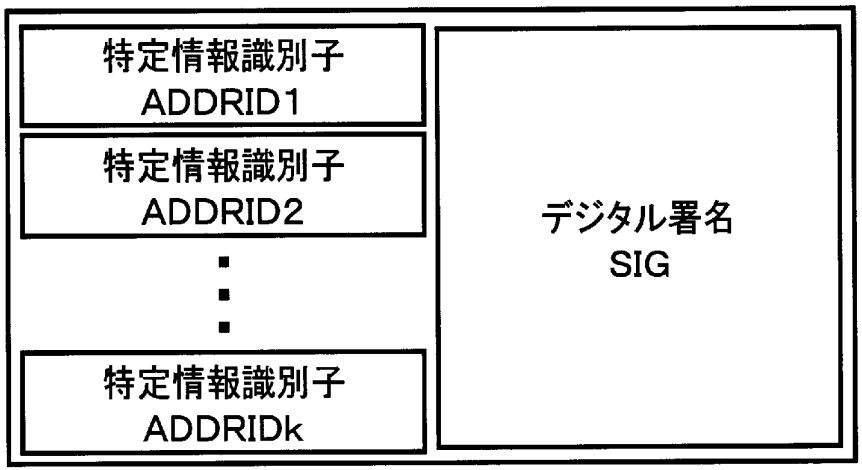
【図５５】

コンテンツ認証情報　CNTAUTHの一例



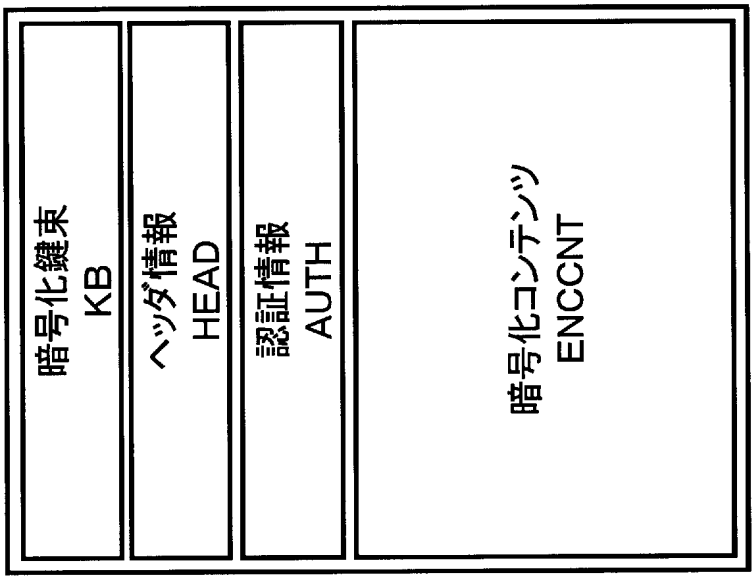
【図５６】

コンテンツ認証情報　CNTAUTHの別の一例



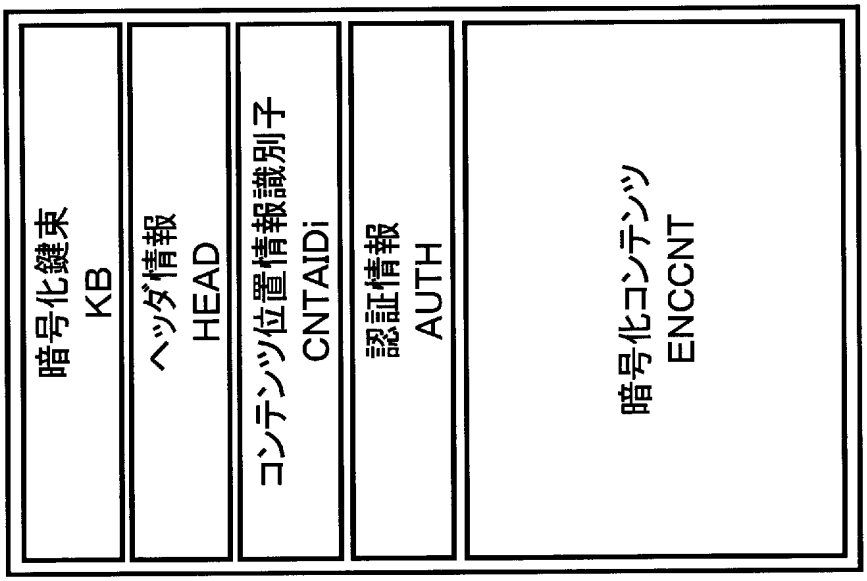
【図５７】

可搬媒体１１に記録されるデータの別の一例

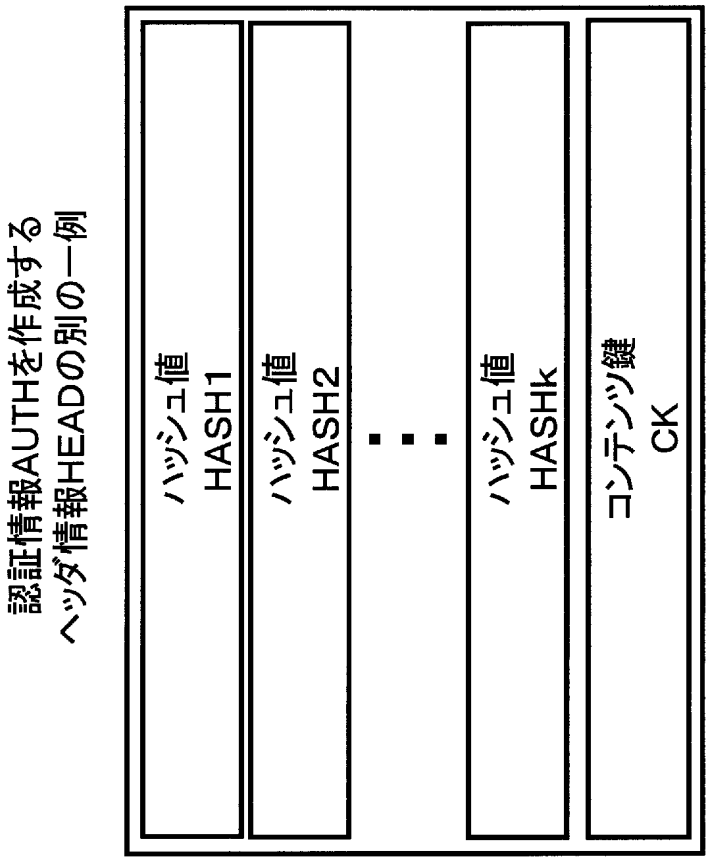


【図５８】

可搬媒体11に記録されるデータの別の一例

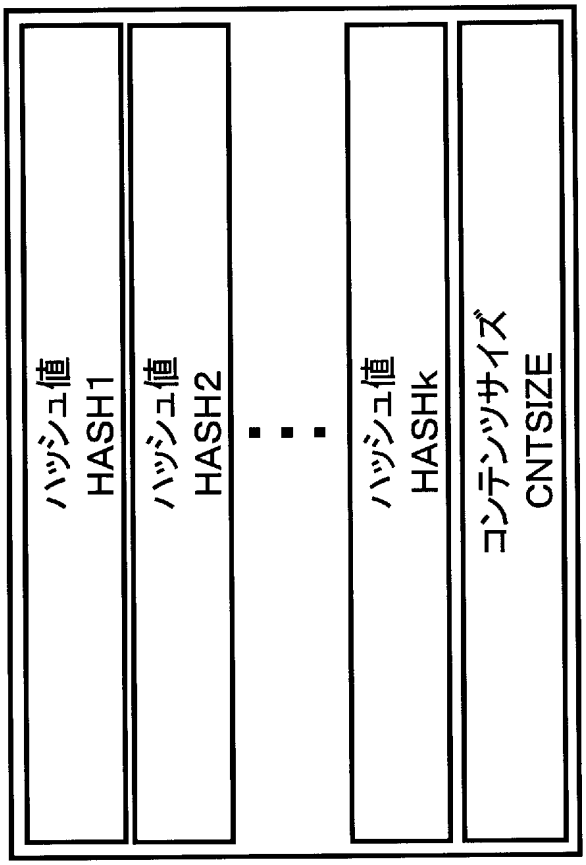


【図５９】

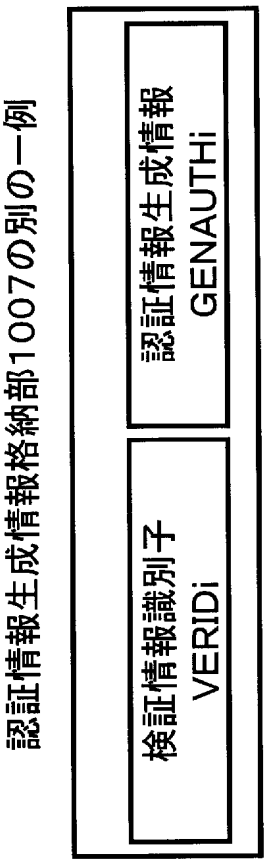

認証情報AUTHを作成する
ヘッダ情報HEADの別の一例
ハッシュ値
HASH1
ハッシュ値
HASH2
ハッシュ値
HASHk
コンテンツ鍵
CK

【図６０】

ヘッダ情報HEADの別の一例

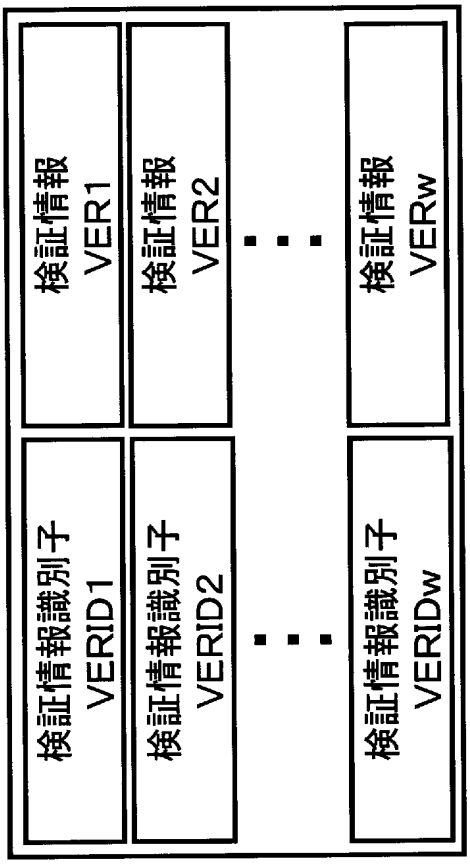


【図６１】



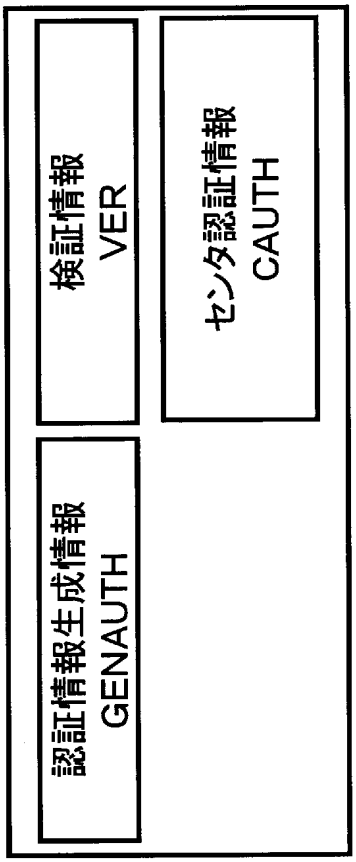
【図６２】

検証情報格納部１２５の別の一例



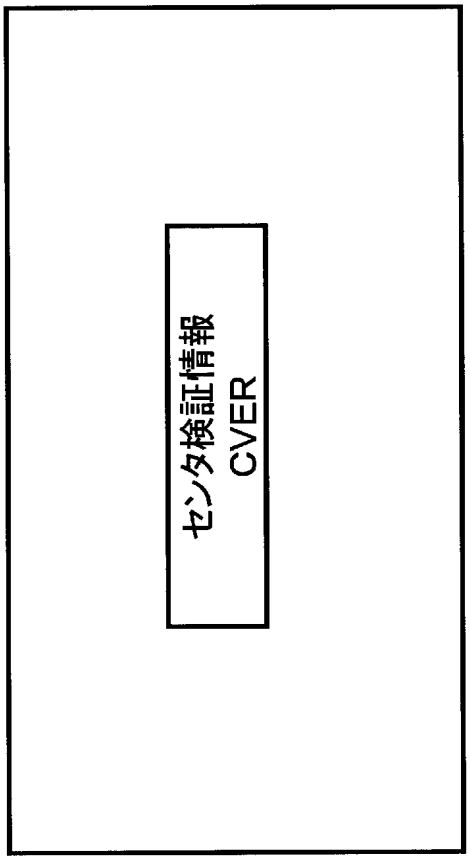
【図６３】

認証情報生成情報格納部1007の別の一例

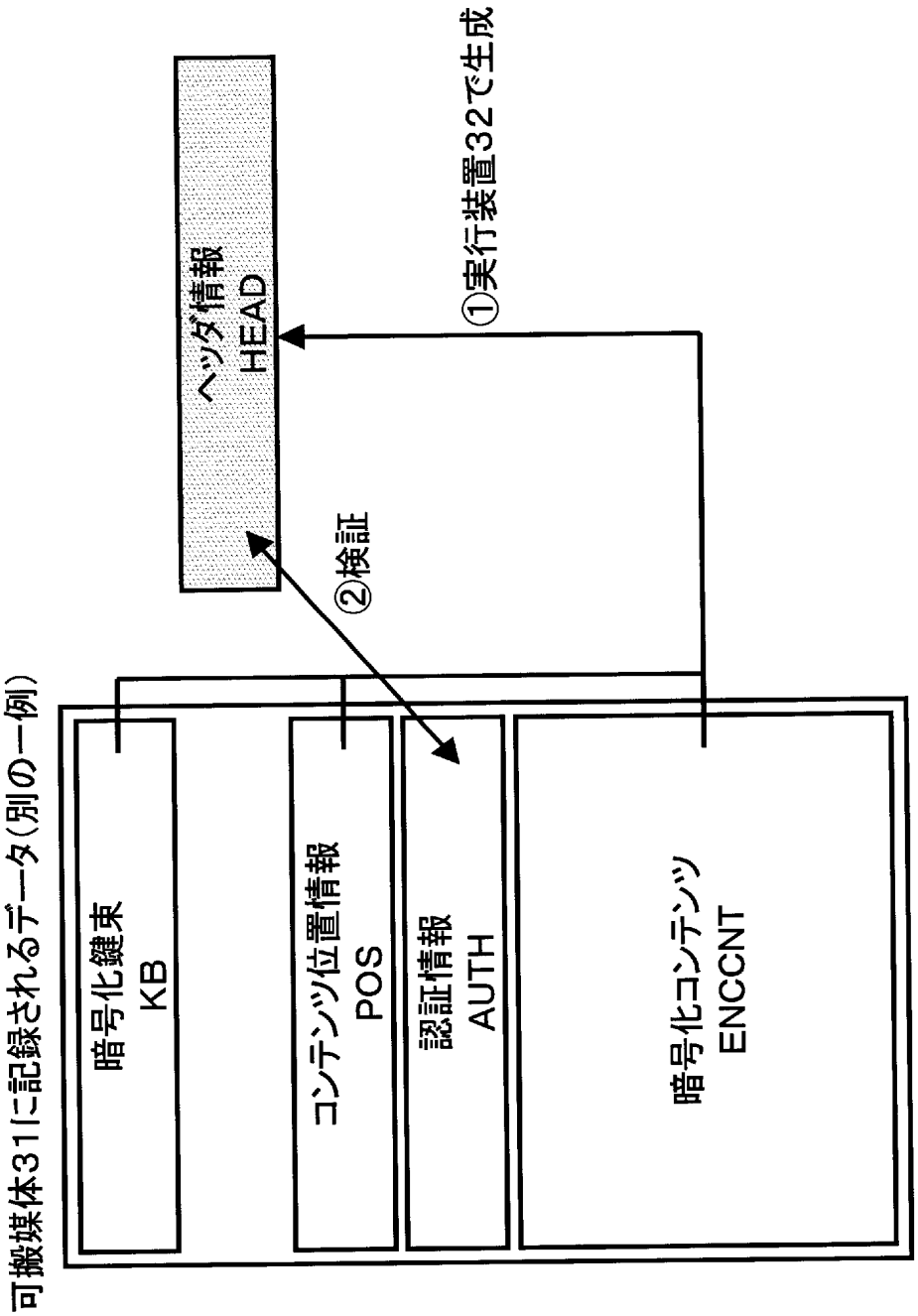


【図６４】

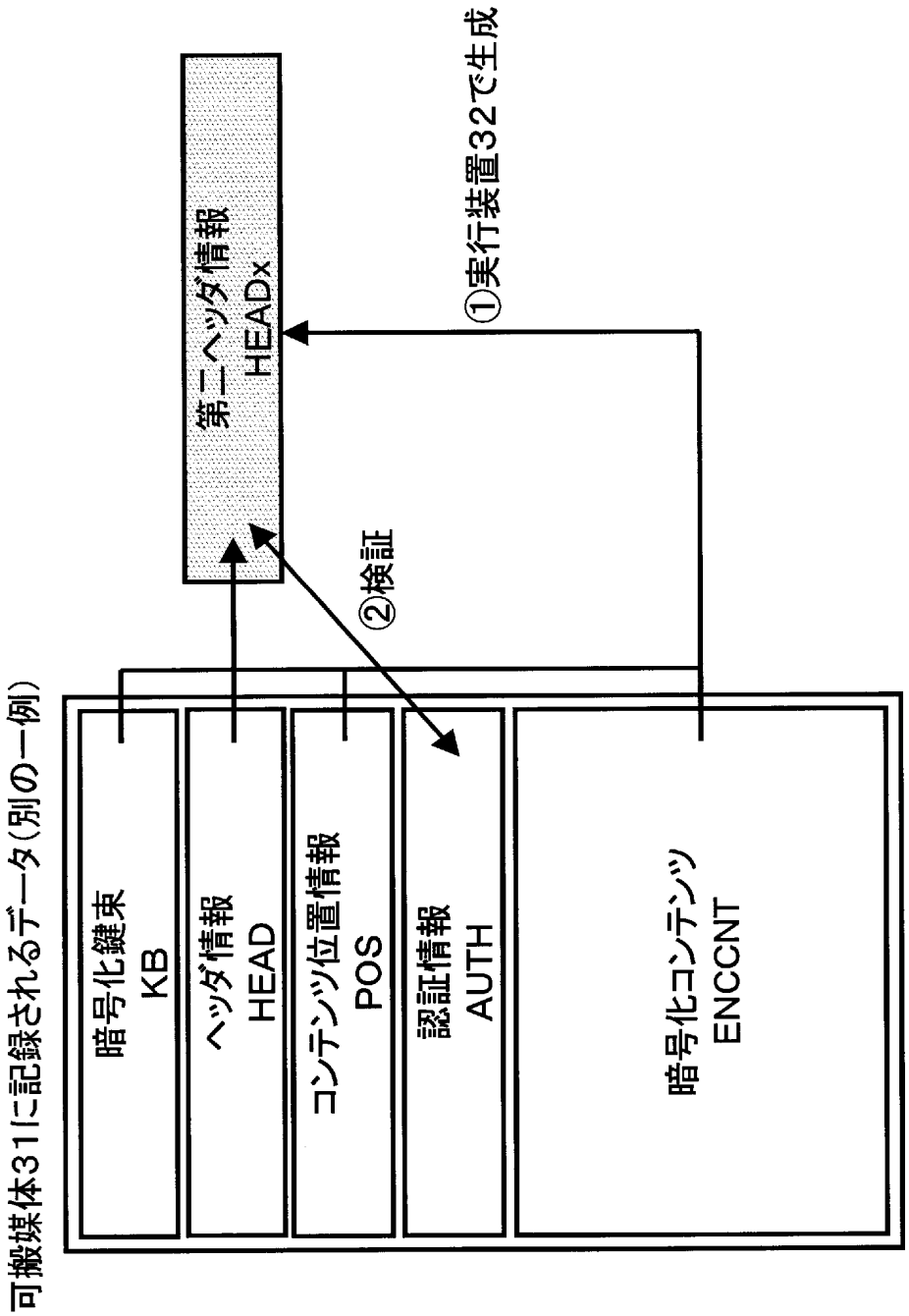
検証情報格納部１２５の別の一例



【図６５】

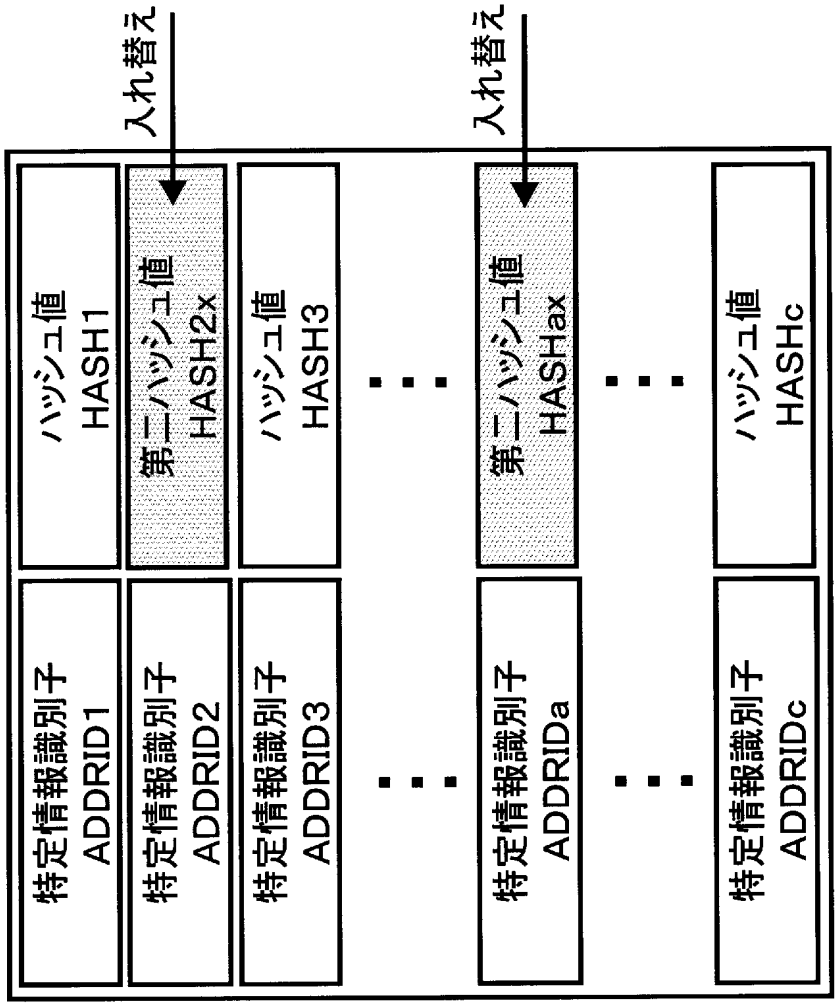

可搬媒体31に記録されるデータ(別の一例)
暗号化鍵束
KB
コンテンツ位置情報
POS
認証情報
AUTH
暗号化コンテンツ
ENCCNT
ヘッダ情報
HEAD
①実行装置32で生成
②検証

【図６６】

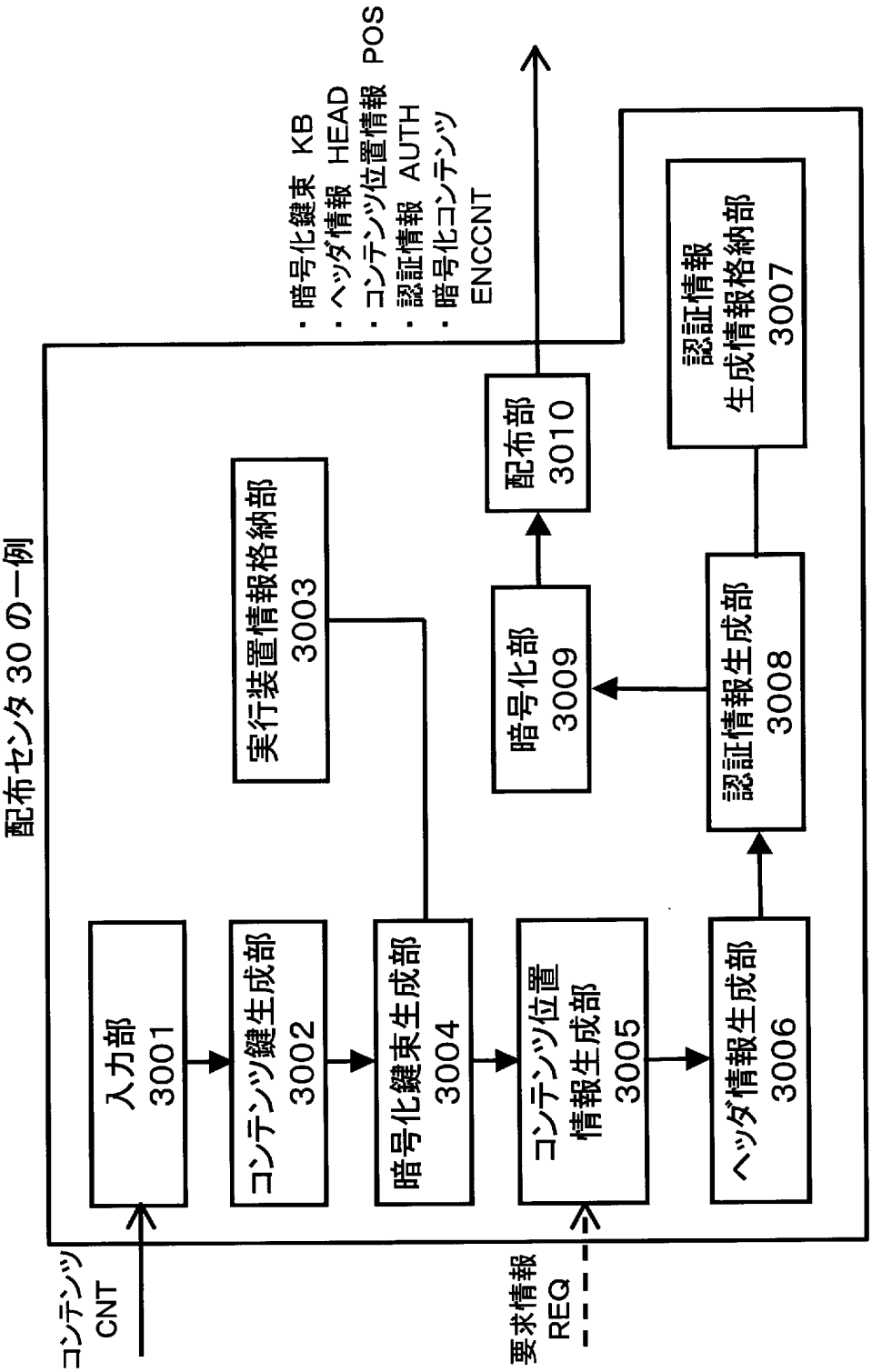

可搬媒体31に記録されるデータ(別の一例)
暗号化鍵束
KB
ヘッダ情報
HEAD
コンテンツ位置情報
POS
認証情報
AUTH
暗号化コンテンツ
ENCCNT
第二ヘッダ情報
HEADx
①実行装置32で生成
②検証

【図６７】

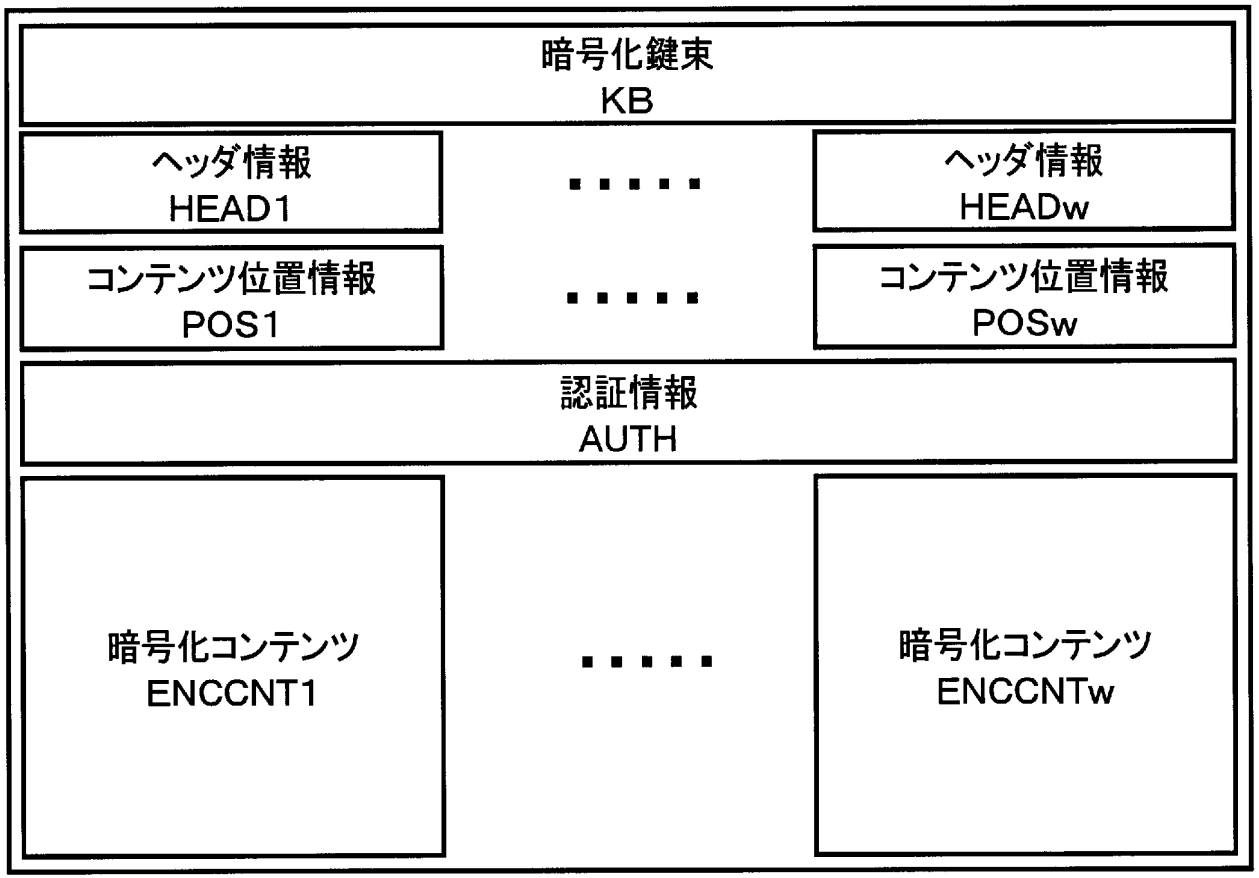
第二ヘッダ情報　HEADxの一例



【図６８】

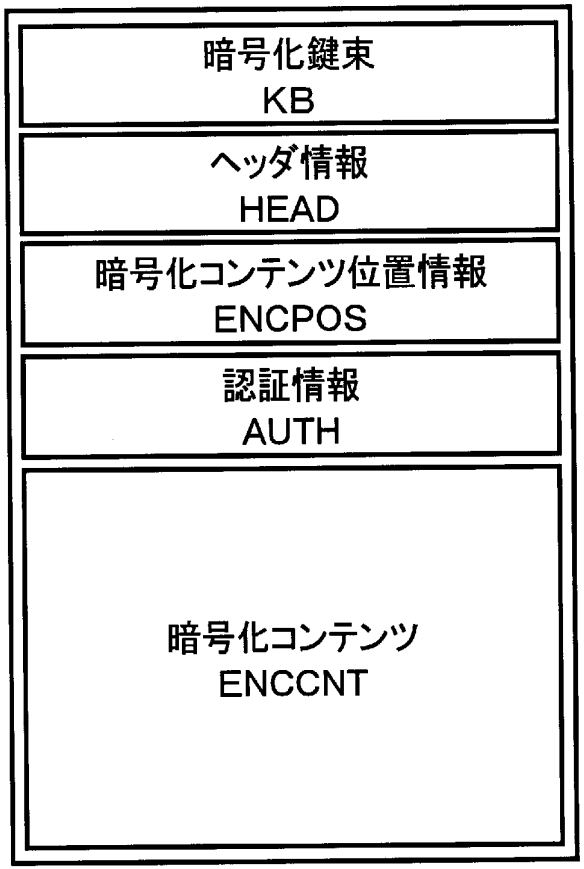

配布センタ 30 の一例
コンテンツ CNT
要求情報 REQ
入力部 3001
コンテンツ鍵生成部 3002
暗号化鍵束生成部 3004
コンテンツ位置情報生成部 3005
ヘッダ情報生成部 3006
実行装置情報格納部 3003
暗号化部 3009
配布部 3010
認証情報生成部 3008
認証情報生成格納部 3007
・暗号化鍵束 KB
・ヘッダ情報 HEAD
・コンテンツ位置情報 POS
・認証情報 AUTH
・暗号化コンテンツ ENCCNT

可搬媒体31に記録されるデータの別の一例



【図７０】

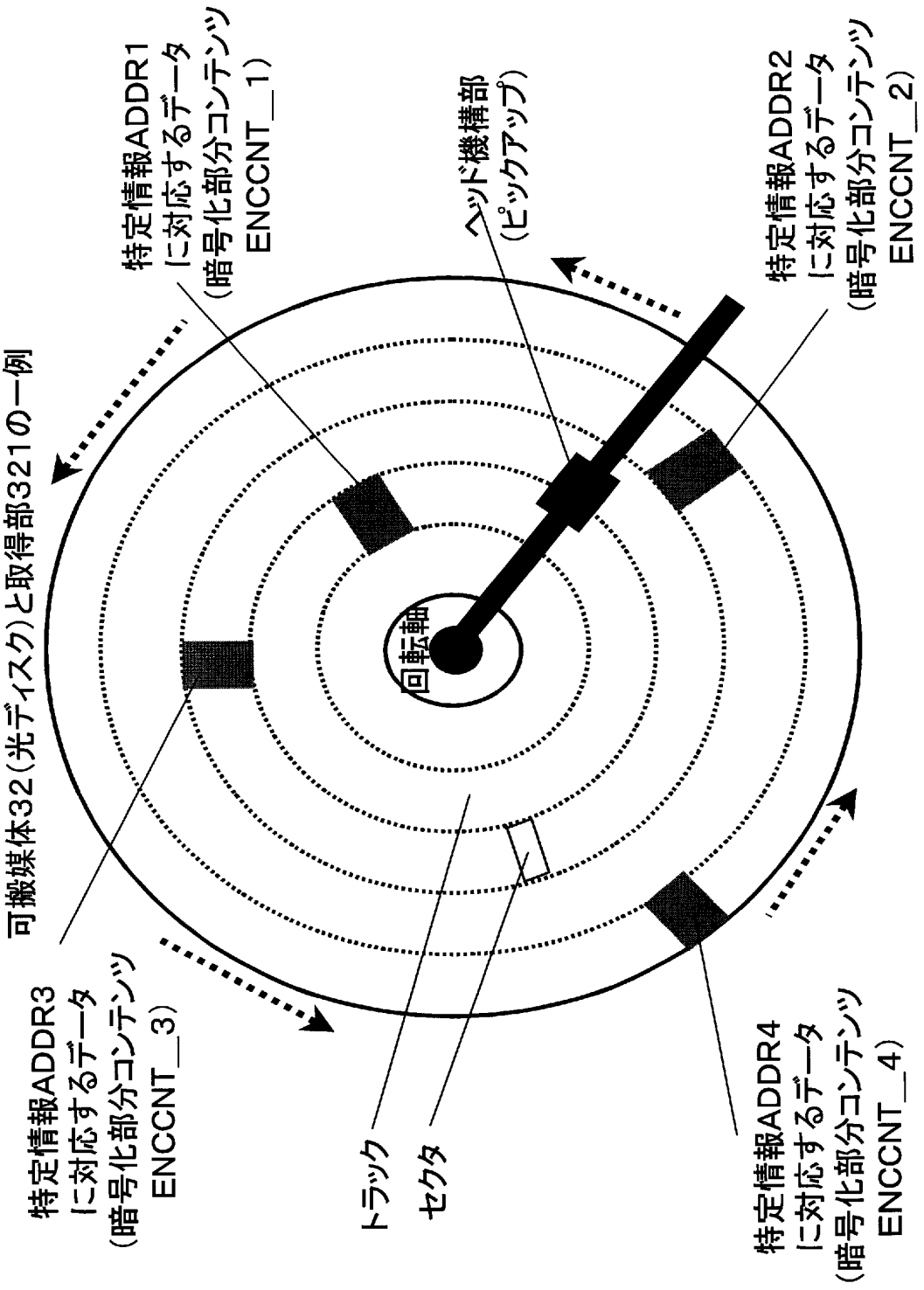
可搬媒体31に記録されるデータの別の一例



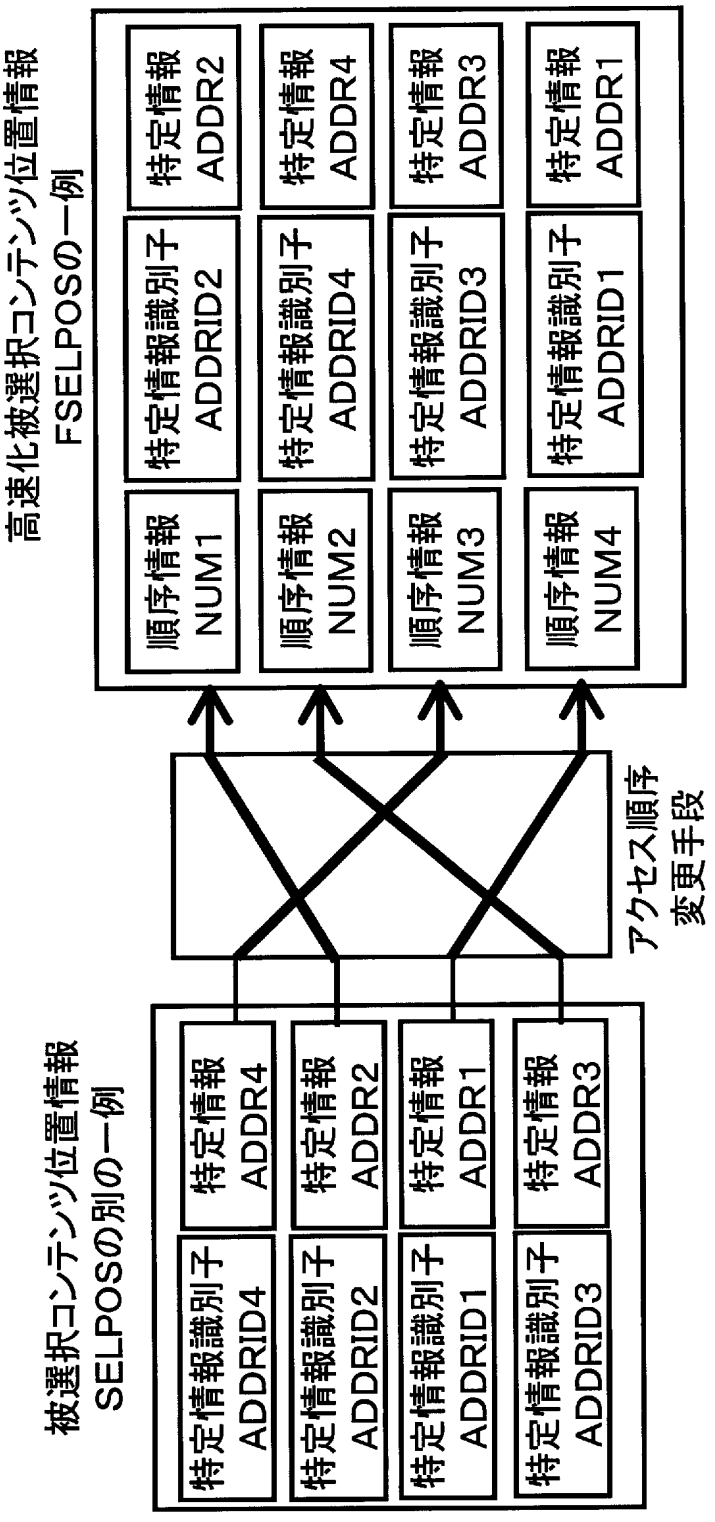
【図７１】

被選択コンテンツ位置情報　SELPOSの別の一例

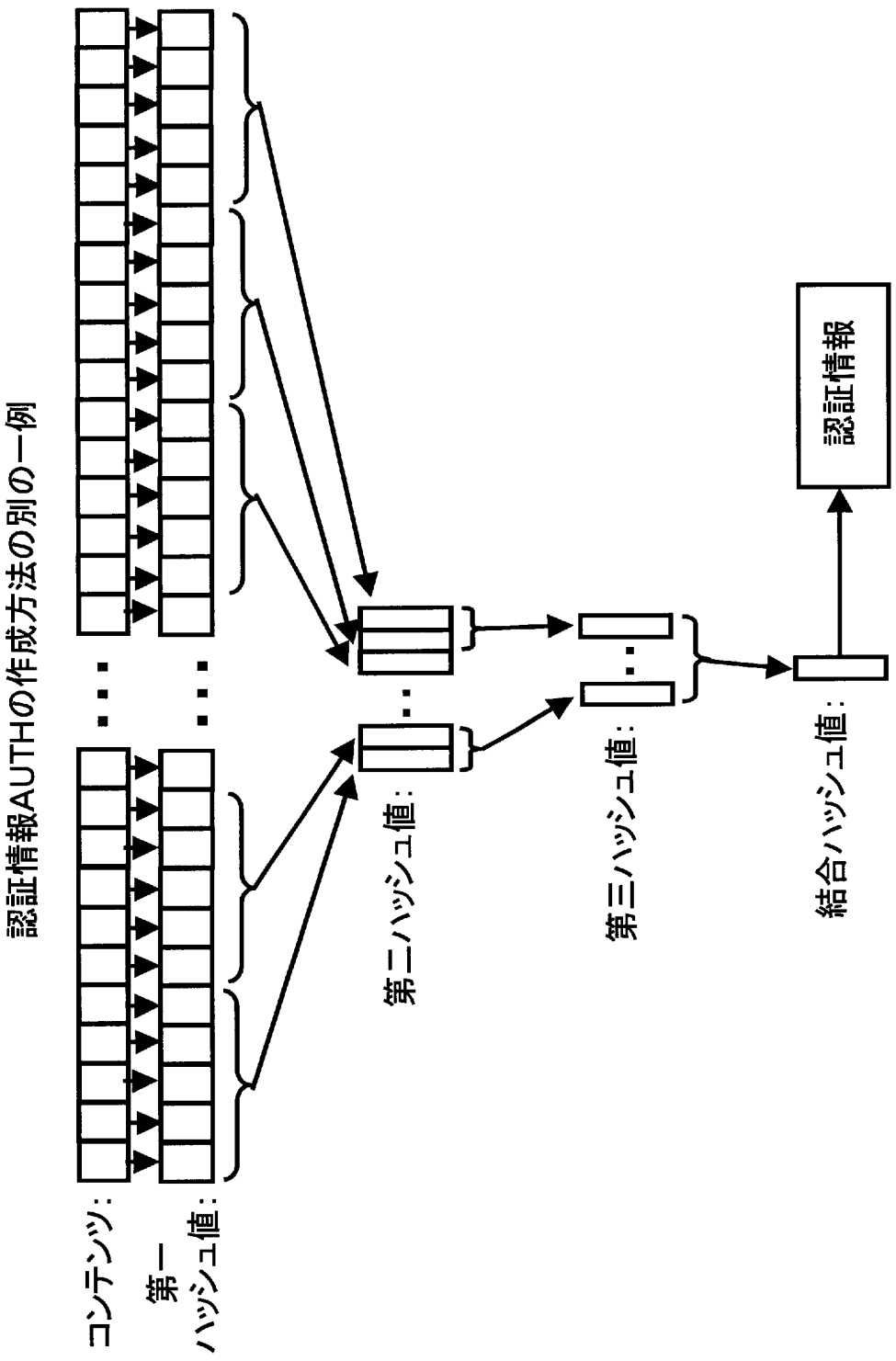
【図７２】


可搬媒体32（光ディスク）と取得部321の一例
特定情報ADDR1
に対応するデータ
（暗号化部分コンテンツ
ENCCNT_1）
ヘッド機構部
（ピックアップ）
特定情報ADDR2
に対応するデータ
（暗号化部分コンテンツ
ENCCNT_2）
特定情報ADDR3
に対応するデータ
（暗号化部分コンテンツ
ENCCNT_3）
回転軸
トラック
セクタ
特定情報ADDR4
に対応するデータ
（暗号化部分コンテンツ
ENCCNT_4）

【図７３】

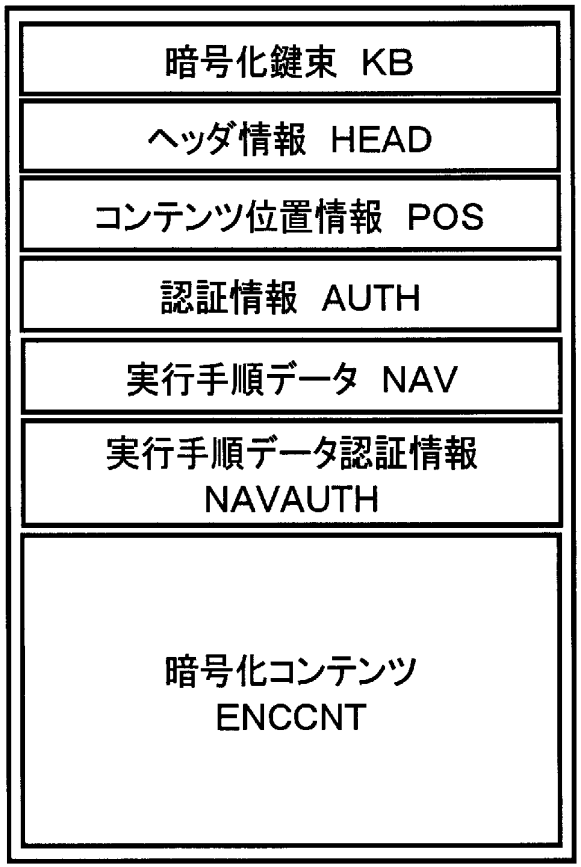

高速化被選択コンテンツ位置情報
FSELPOSの一例
順序情報
NUM1
特定情報識別子
ADDRID2
特定情報
ADDR2
順序情報
NUM2
特定情報識別子
ADDRID4
特定情報
ADDR4
順序情報
NUM3
特定情報識別子
ADDRID3
特定情報
ADDR3
順序情報
NUM4
特定情報識別子
ADDRID1
特定情報
ADDR1
アクセス順序
変更手段
被選択コンテンツ位置情報
SELPOSの別の一例
特定情報識別子
ADDRID4
特定情報
ADDR4
特定情報識別子
ADDRID2
特定情報
ADDR2
特定情報識別子
ADDRID1
特定情報
ADDR1
特定情報識別子
ADDRID3
特定情報
ADDR3

【図７４】

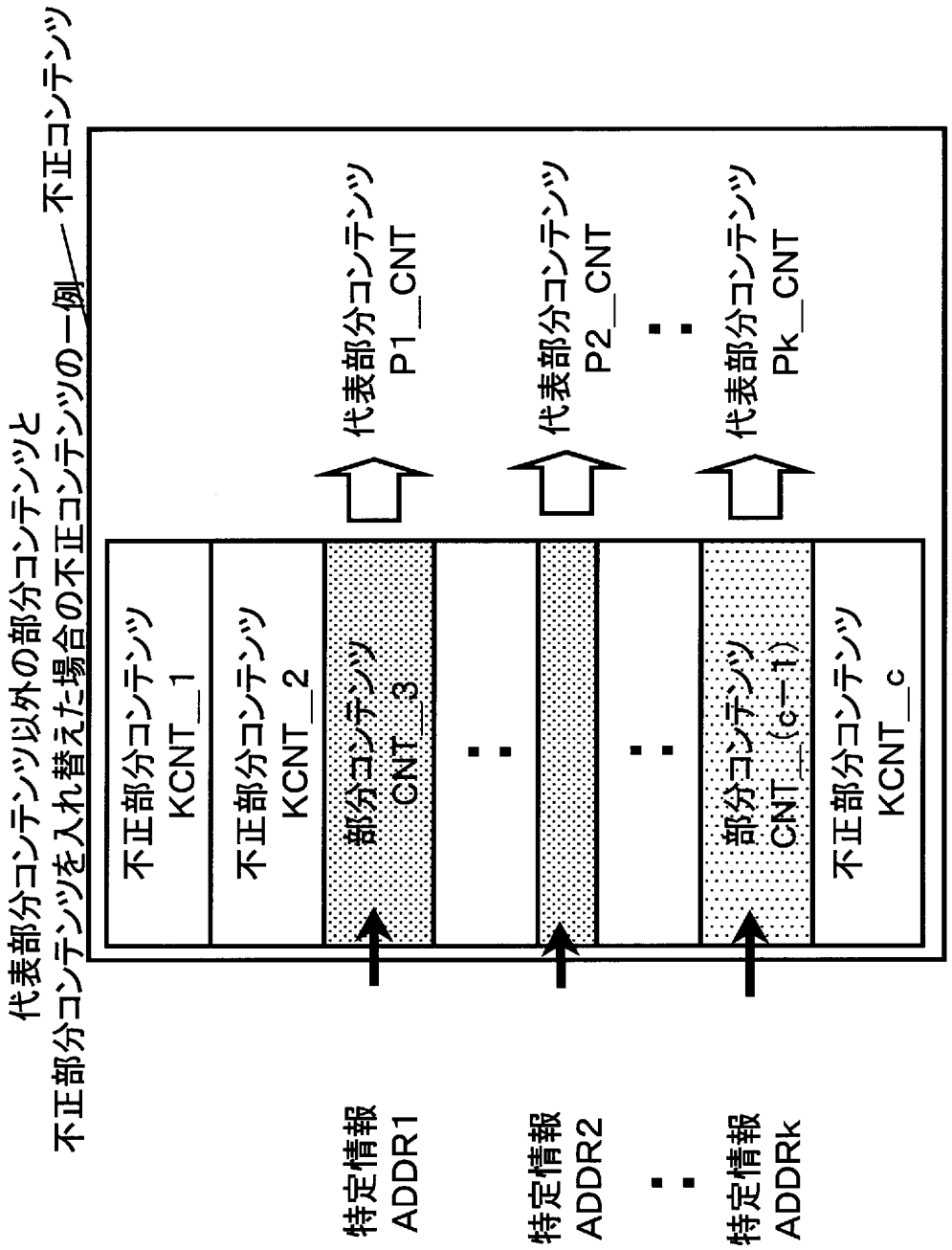

認証情報AUTHの作成方法の別の一例
コンテンツ：
第一
ハッシュ値：
第二ハッシュ値：
第三ハッシュ値：
結合ハッシュ値：
認証情報

【図７５】

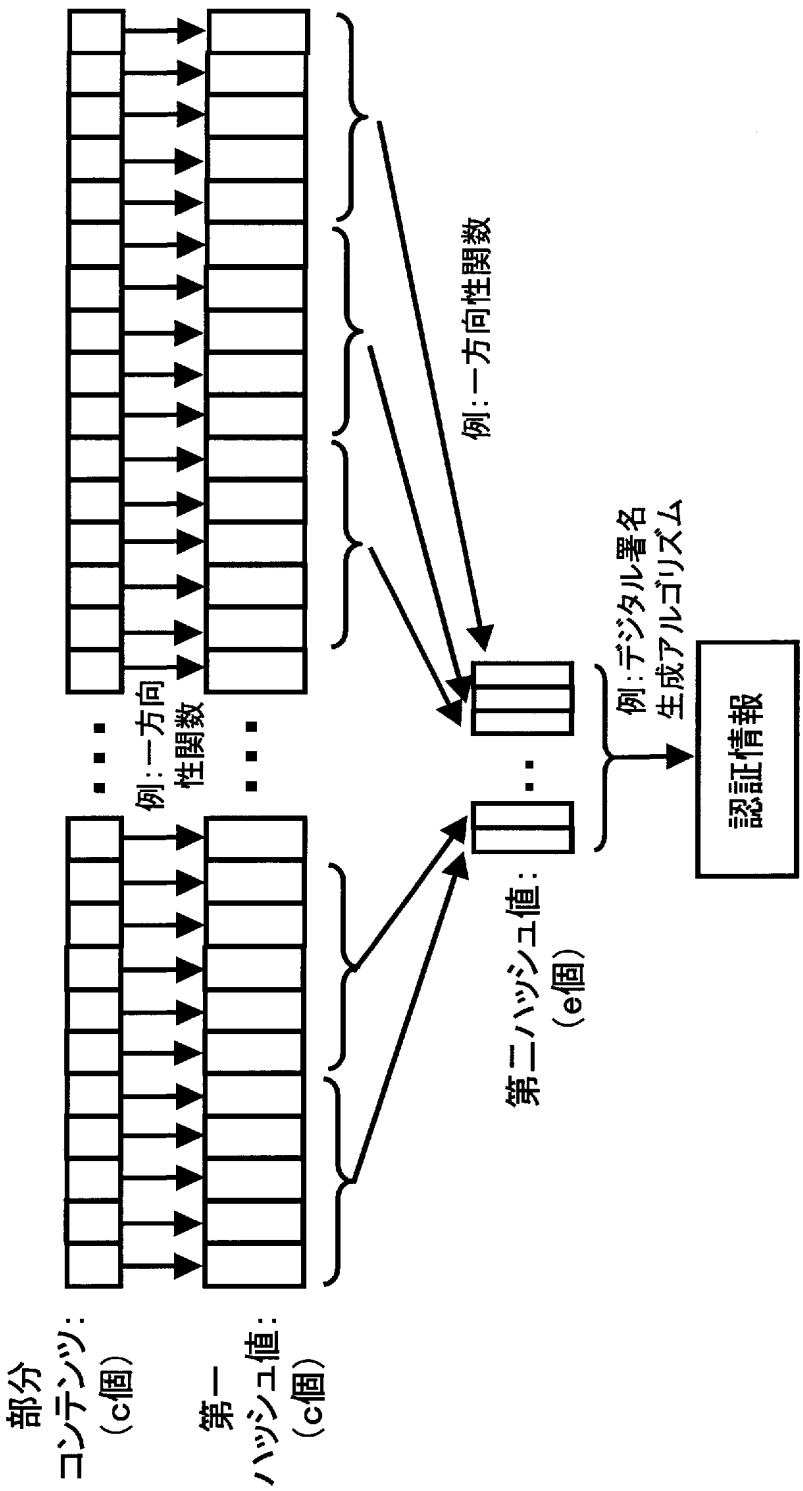
可搬媒体11に記録されるデータの別の一例



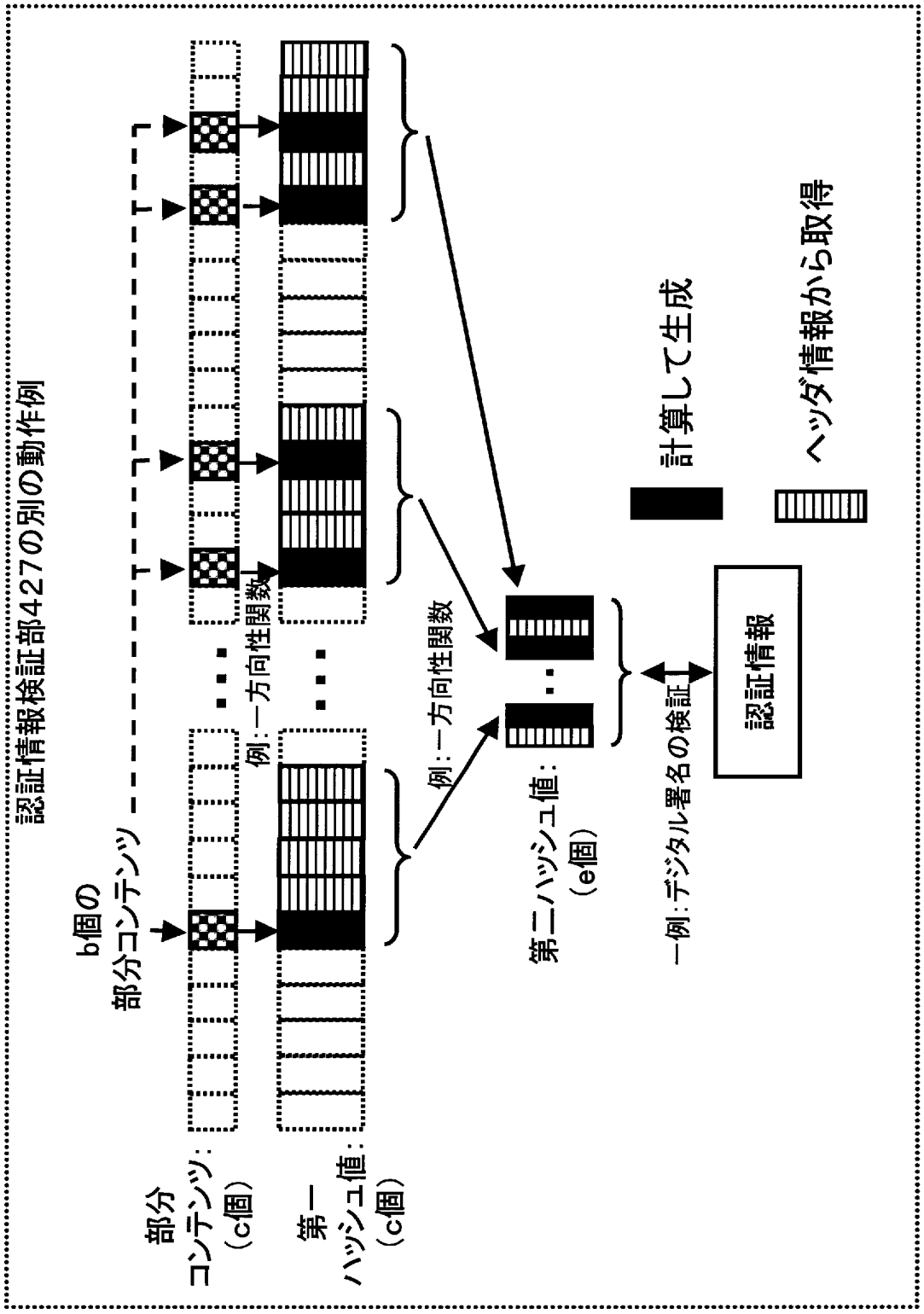
【図７６】


代表部分コンテンツ以外の部分コンテンツと
不正部分コンテンツを入れ替えた場合の不正コンテンツの一例
不正コンテンツ
不正部分コンテンツ
KCNT_1
不正部分コンテンツ
KCNT_2
部分コンテンツ
CNT_3
部分コンテンツ
CNT_(c-1)
不正部分コンテンツ
KCNT_c
代表部分コンテンツ
P1_CNT
代表部分コンテンツ
P2_CNT
代表部分コンテンツ
Pk_CNT
特定情報
ADDR1
特定情報
ADDR2
特定情報
ADDRk

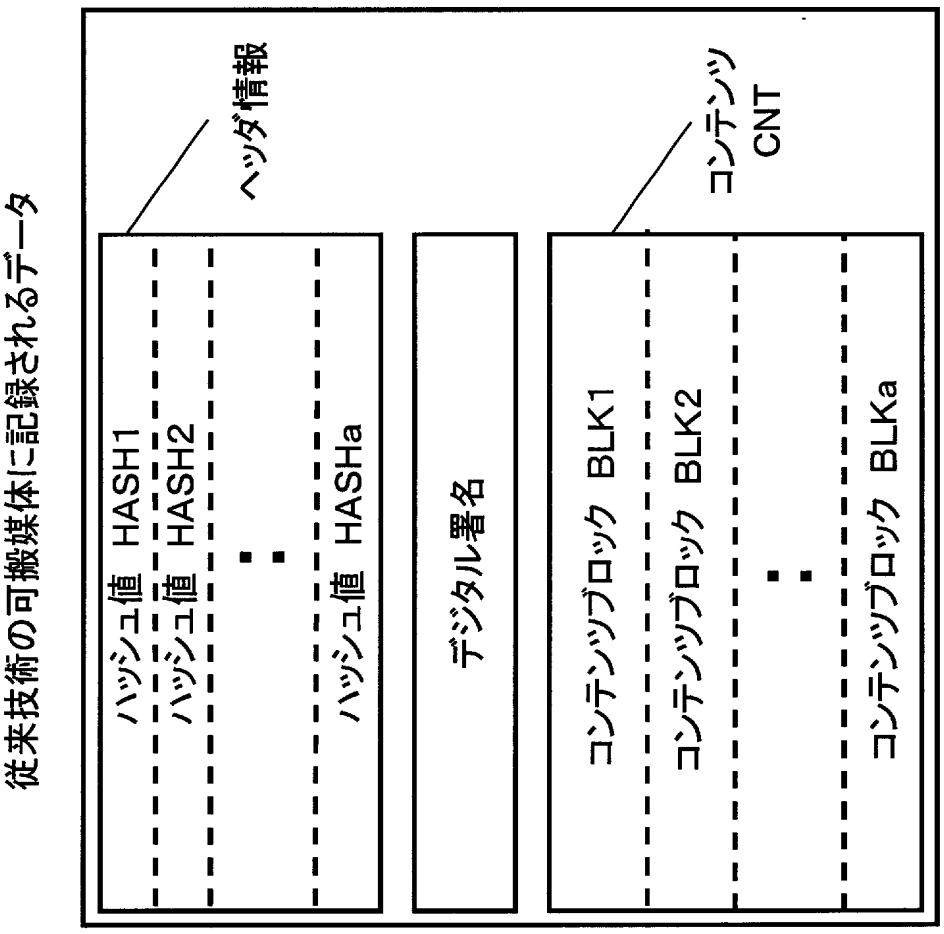
【図７７】


認証情報AUTHの作成方法の別の一例
部分
コンテンツ：
（c個）
第一
ハッシュ値：
（c個）
例：一方向
性関数
第二ハッシュ値：
（e個）
例：一方向性関数
例：デジタル署名
生成アルゴリズム
認証情報

【図７８】


認証情報検証部427の別の動作例
b個の
部分コンテンツ
部分
コンテンツ:
(c個)
例:一方向性関数
第一
ハッシュ値:
(c個)
例:一方向性関数
第二ハッシュ値:
(e個)
一例:デジタル署名の検証
認証情報
計算して生成
ヘッダ情報から取得

【図７９】


従来技術の可搬媒体に記録されるデータ
ヘッダ情報
ハッシュ値 HASH1
ハッシュ値 HASH2
ハッシュ値 HASHa
デジタル署名
コンテンツ
CNT
コンテンツブロック BLK1
コンテンツブロック BLK2
コンテンツブロック BLKa

【書類名】要約書
【要約】
【課題】　実行装置において不正コンテンツかどうか検知する処理において、コンテンツ実行中の処理負荷が大きかった。
【解決手段】　まずコンテンツＣＮＴを構成するｃ個の部分コンテンツＣＮＴ―１、・・・、ＣＮＴ―ｃの中から、一つの部分コンテンツを選択し、それを代表部分コンテンツＰ１―ＣＮＴとする。そして、その代表部分コンテンツＰ１―ＣＮＴを指し示す特定情報をＡＤＤＲ１とする。そして、続けて、ｋ－１個の代表部分コンテンツＰ２―ＣＮＴ、・・・、Ｐｋ―ＣＮＴを選択し、その代表部分コンテンツに対応する特定情報をＡＤＤＲ２、・・・、ＡＤＤＲｋとする。
【選択図】　図６

出願人履歴

０００００５８２１
19900828
新規登録

大阪府門真市大字門真１００６番地
松下電器産業株式会社